

PCT/JP 01/00346

19.01.01

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JP01/346

EKV

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 1月25日

出 願 番 号

Application Number:

特願2000-015551

出 願 人

Applicant (s):

ソニー株式会社

REC'D 05 FEB 2001

WIPO PCT

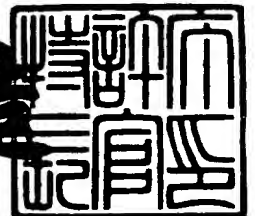
PRIORITY
DOCUMENT

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年12月 8日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3102451

【書類名】 特許願

【整理番号】 99008895

【提出日】 平成12年 1月25日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明の名称】 データ処理装置、データ処理システム、およびデータ処理方法、並びにプログラム提供媒体

【請求項の数】 22

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 白井 太三

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 秋下 徹

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 石橋 義人

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置、データ処理システム、およびデータ処理方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項1】

データ処理装置において、

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理部と、

前記暗号処理に適用する鍵を生成するためのマスター鍵を格納した記憶部とを有し、

前記暗号処理部は、前記暗号処理を実行するに必要な個別鍵を、前記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する構成を有することを特徴とするデータ処理装置。

【請求項2】

前記データ処理装置は、記憶媒体または通信媒体を介する転送データに関する暗号処理を行なうデータ処理装置であり、

前記記憶部は、前記転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} を格納し、

前記暗号処理部は、

前記記憶部に格納された配送鍵生成用マスター鍵 MK_{dis} と、前記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行して、前記転送データの配送鍵 K_{dis} を生成する構成を有することを特徴とする請求項1に記載のデータ処理装置。

【請求項3】

前記データ処理装置は、転送データの転送先あるいは転送元となる外部接続装置の認証処理を行なうデータ処理装置であり、

前記記憶部は、前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成用マスター鍵 MK_{ake} を格納し、

前記暗号処理部は、

前記記憶部に格納された認証鍵生成用マスター鍵MKakeと、前記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、前記外部接続装置の認証鍵Kakeを生成する構成を有することを特徴とする請求項1に記載のデータ処理装置。

【請求項4】

前記データ処理装置は、データに対する署名処理を実行するデータ処理装置であり、

前記記憶部は、前記データ処理装置のデータ処理装置署名鍵Kdevを生成する署名鍵生成用マスター鍵MKdevを格納し、

前記暗号処理部は、

前記記憶部に格納された署名鍵生成用マスター鍵MKdevと、前記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、前記データ処理装置のデータ処理装置署名鍵Kdevを生成する構成を有することを特徴とする請求項1に記載のデータ処理装置。

【請求項5】

暗号処理を実行するに必要な個別鍵を、前記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する個別鍵生成処理は、

暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、前記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする請求項1に記載のデータ処理装置。

【請求項6】

前記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする請求項5に記載のデータ処理装置。

【請求項7】

複数のデータ処理装置から構成されるデータ処理システムにおいて、

前記複数のデータ処理装置の各々が、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理に適用する鍵を生成するための共通のマスター鍵を有し、

前記複数のデータ処理装置の各々が、前記マスター鍵と、暗号処理対象の装置

またはデータの識別データに基づいて前記暗号処理を実行するに必要な共通の個別鍵を生成する構成を有することを特徴とするデータ処理システム。

【請求項 8】

前記複数のデータ処理装置は、

コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置によって構成され、

コンテンツデータ提供装置およびコンテンツデータ利用装置の双方が、前記コンテンツデータ提供装置およびコンテンツデータ利用装置間における流通コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵を有し、

前記コンテンツデータ提供装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、

前記コンテンツデータ利用装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行する構成を有することを特徴とする請求項 7 に記載のデータ処理システム。

【請求項 9】

前記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と前記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、

前記コンテンツデータ利用装置は、前記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも 1 つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号可能とした構成を有することを特徴とする請求項 8 に記載のデータ処理システム。

【請求項 10】

前記複数のデータ処理装置の各々に、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するための同一のコンテンツ鍵生成用マスター鍵を格納し、

前記複数のデータ処理装置の 1 つのデータ処理装置 A において、前記コンテンツ鍵生成用マスター鍵と、該データ処理装置 A の装置識別子とに基づいて生成されたコンテンツ鍵により暗号化され記憶媒体に格納されたコンテンツデータを、

異なるデータ処理装置 B において、前記同一のコンテンツ鍵生成用マスター鍵と、前記データ処理装置 A の装置識別子とに基づいてコンテンツ鍵を生成し、該生成したコンテンツ鍵に基づいて、前記データ処理装置 A において前記記憶媒体に格納した暗号化コンテンツデータの復号処理を実行する構成としたことを特徴とする請求項 7 に記載のデータ処理システム。

【請求項 1 1】

前記複数のデータ処理装置は、

ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとによって構成され、

前記ホストデバイスおよびスレーブデバイスの双方が、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵生成用マスターを有し、

前記スレーブデバイスは、前記認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成してスレーブデバイス内メモリに格納し、

前記ホストデバイスは、前記認証鍵生成用マスター鍵と、前記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行する構成を有することを特徴とする請求項 7 に記載のデータ処理システム。

【請求項 1 2】

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理を実行するデータ処理方法において、

暗号処理を実行するに必要な個別鍵を、前記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

前記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、

を有することを特徴とするデータ処理方法。

【請求項 1 3】

前記データ処理方法において実行するデータ処理は、記憶媒体または通信媒体を介する転送データに関する暗号処理であり、

前記鍵生成ステップは、

転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} と、前記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行し、前記転送データの配送鍵 K_{dis} を生成する配送鍵生成ステップであり、

前記暗号処理ステップは、

前記配送鍵生成ステップにおいて生成した配送鍵 K_{dis} に基づいて転送データの暗号処理を実行するステップであることを特徴とする請求項 1 2 に記載のデータ処理方法。

【請求項 1 4】

前記データ処理方法において実行するデータ処理は、転送データの転送先あるいは転送元となる外部接続装置の認証処理であり、

前記鍵生成ステップは、

前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成用マスター鍵 MK_{ake} と、前記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成ステップであり、

前記暗号処理ステップは、

前記認証鍵生成ステップにおいて生成した認証鍵 K_{ake} に基づいて外部接続装置の認証処理を実行するステップであることを特徴とする請求項 1 2 に記載のデータ処理方法。

【請求項 1 5】

前記データ処理装置において実行するデータ処理は、データに対する署名処理

であり、

前記鍵生成ステップは、

前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成用マスター鍵 MK_{dev} と、前記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成ステップであり、

前記暗号処理ステップは、

前記署名鍵生成ステップにおいて生成した署名鍵 K_{dev} に基づいてデータに対する署名処理を実行するステップであることを特徴とする請求項 12 に記載のデータ処理方法。

【請求項 16】

前記鍵生成ステップは、

暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、前記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする請求項 12 に記載のデータ処理方法。

【請求項 17】

前記暗号処理は DES アルゴリズムを適用した暗号処理であることを特徴とする請求項 16 に記載のデータ処理方法。

【請求項 18】

コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置とからなるデータ処理システムにおけるデータ処理方法であり、

前記コンテンツデータ提供装置は、コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、

前記コンテンツデータ利用装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行することを特徴とする

データ処理方法。

【請求項19】

前記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と前記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、

前記コンテンツデータ利用装置は、前記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号することを特徴とする請求項18に記載のデータ処理方法。

【請求項20】

複数のデータ処理装置によって構成されるデータ処理システムにおけるデータ処理方法であり、

前記複数のデータ処理装置中の1つのデータ処理装置Aにおいて、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するためのコンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化されたコンテンツデータを記憶媒体に格納するステップと、

異なるデータ処理装置Bにおいて、前記データ処理装置Aと同一の前記コンテンツ鍵生成用マスター鍵と前記データ処理装置Aの装置識別子とに基づいて前記コンテンツ鍵と同一のコンテンツ鍵を生成するステップと、

前記データ処理装置Bにおいて生成したコンテンツ鍵により前記記憶媒体に格納したコンテンツデータの復号を行なうステップと、

を有することを特徴とするデータ処理方法。

【請求項21】

ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとからなるデータ処理システムにおけるデータ処理方法であり、

前記スレーブデバイスは、ホストデバイスとスレーブデバイス間の認証処理に

適用する認証鍵を生成するための認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成し、生成した認証鍵を該スレーブデバイス内のメモリに格納し、

前記ホストデバイスは、前記認証鍵生成用マスター鍵と、前記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行することを特徴とするデータ処理方法。

【請求項 2 2】

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

暗号処理を実行するに必要な個別鍵を、前記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

前記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、

を含むことを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データ処理装置、データ処理システム、およびデータ処理方法、並びにプログラム提供媒体に関し、さらに詳細には、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の各種の暗号処理を実行するデータ処理装置において暗号処理に必要な個別鍵を、各個別鍵に対応したマスター鍵によって生成することにより、セキュリティを高めることを可能としたデータ処理装置、データ処理システム、およびデータ処理方法に関する。

【0 0 0 2】

本発明は、DVD、CD等の記憶媒体、あるいはCATV、インターネット、衛星通信等の有線、無線各通信手段等の経路で入手可能な音声、画像、ゲーム、

プログラム等の各種コンテンツを、ユーザの所有する記録再生器において再生し、専用の記録デバイス、例えばメモリカード、ハードディスク、CD-R等に格納するとともに、記録デバイスに格納されたコンテンツを利用する際、コンテンツ配信側の希望する利用制限を付す構成を実現するとともに、この配布されたコンテンツを、正規ユーザ以外の第三者に不正利用されないようにセキュリティを確保する構成および方法に関する。

【0003】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、ゲーム機器等の記録再生機器に付属する記録デバイス、例えばメモリカード、ハードディスク等に格納することが可能であり、一旦格納された後は、格納媒体からの再生により利用可能となる。

【0004】

従来のビデオゲーム機器、PC等の情報機器において使用されるメモリカード装置の主な構成要素は、動作制御のための制御手段と、制御手段に接続され情報機器本体に設けられたスロットに接続するためのコネクタと、制御手段に接続されデータを記憶するための不揮発性メモリ等である。メモリカードに備えられた不揮発性メモリはEEPROM、フラッシュメモリ等によって構成される。

【0005】

このようなメモリカードに記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により不揮発性メモリから呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【0006】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテ

ンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【0007】

ユーザに対する利用制限を実現する1つの手法が、配布コンテンツの暗号化処理である。すなわち、例えばインターネット等を介して暗号化された音声データ、画像データ、ゲームプログラム等の各種コンテンツを配布するとともに、正規ユーザであると確認された者に対してのみ、配布された暗号化コンテンツを復号する手段、すなわち復号鍵を付与する構成である。

【0008】

暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。

【0009】

暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その1つの例としていわゆる共通鍵暗号化方式と呼ばれている方式がある。共通鍵暗号化方式は、データの暗号化処理に用いる暗号化鍵とデータの復号化に用いる復号化鍵を共通のものとして、正規のユーザにこれら暗号化処理、復号化に用いる共通鍵を付与して、鍵を持たない不正ユーザによるデータアクセスを排除するものである。この方式の代表的な方式にDES（データ暗号標準：Data encryption standard）がある。

【0010】

上述の暗号化処理、復号化に用いられる暗号化鍵、復号化鍵は、例えばあるパスワード等に基づいてハッシュ関数等の一方向性関数を適用して得ることができる。一方向性関数とは、その出力から逆に入力を求めるのは非常に困難となる関数である。例えばユーザが決めたパスワードを入力として一方向性関数を適用し

て、その出力に基づいて暗号化鍵、復号化鍵を生成するものである。このようにして得られた暗号化鍵、復号化鍵から、逆にそのオリジナルのデータであるパスワードを求めることは実質上不可能となる。

【0011】

また、暗号化するとき使用する暗号化鍵による処理と、復号するとき使用する復号化鍵の処理とを異なるアルゴリズムとした方式がいわゆる公開鍵暗号化方式と呼ばれる方式である。公開鍵暗号化方式は、不特定のユーザが使用可能な公開鍵を使用する方法であり、特定個人に対する暗号化文書を、その特定個人が発行した公開鍵を用いて暗号化処理を行なう。公開鍵によって暗号化された文書は、その暗号化処理に使用された公開鍵に対応する秘密鍵によってのみ復号処理が可能となる。秘密鍵は、公開鍵を発行した個人のみが所有するので、その公開鍵によって暗号化された文書は秘密鍵を持つ個人のみが復号することができる。公開鍵暗号化方式の代表的なものにはRSA (Rivest-Shamir-Adleman) 暗号がある。

【0012】

このような暗号化方式を利用することにより、暗号化コンテンツを正規ユーザに対してのみ復号可能とするシステムが可能となる。これらの暗号方式を採用した従来のコンテンツ配布構成について図1を用いて簡単に説明する。

【0013】

図1は、PC (パーソナルコンピュータ)、ゲーム機器等の再生手段10において、DVD、CD30、インターネット40等のデータ提供手段から取得したプログラム、音声データ、映像データ等 (コンテンツ (Content)) を再生するとともに、DVD、CD30、インターネット40等から取得したデータをフロッピーディスク、メモ리카ード、ハードディスク等の記憶手段20に記憶可能とした構成例を示すものである。

【0014】

プログラム、音声データ、映像データ等のコンテンツは、暗号化処理がなされ、再生手段10を有するユーザに提供される。正規ユーザは、暗号化データとともに、その暗号化、復号化鍵である鍵データを取得する。

【0015】

再生手段10はCPU12を有し、入力データの再生処理を再生処理部14で実行する。再生処理部14は、暗号化データの復号処理を実行して、提供されたプログラムの再生、音声データ、画像データ等コンテンツ再生を行なう。

【0016】

正規ユーザは、提供されたプログラムを、再度使用するために記憶手段20にプログラム／データ等、コンテンツの保存処理を行なう。再生手段10には、このコンテンツ保存処理を実行するための保存処理部13を有する。保存処理部13は、記憶手段20に記憶されたデータの不正使用を防止するため、データに暗号化処理を施して保存処理を実行する。

【0017】

コンテンツを暗号化する際には、コンテンツ暗号用鍵を用いる。保存処理部13は、コンテンツ暗号用鍵を用いて、コンテンツを暗号化し、それをFD（フロッピーディスク）、メモ리카ード、ハードディスク等の記憶手段20の記憶部21に記憶する。

【0018】

ユーザは、記憶手段20から格納コンテンツを取り出して再生する場合には、記憶手段20から、暗号化データを取り出して、再生手段10の再生処理部14において、コンテンツ復号用の鍵、すなわち復号化鍵を用いて復号処理を実行して暗号化データから復号データを取得して再生する。

【0019】

図1に示す従来の構成例に従えば、フロッピーディスク、メモ리카ード等の記憶手段20では格納コンテンツが暗号化されているため、外部からの不正読み出しは防止可能となる。しかしながら、このフロッピーディスクを他のPC、ゲーム機器等の情報機器の再生手段で再生して利用しようとする、同じコンテンツ鍵、すなわち暗号化されたコンテンツを復号するための同じ復号化鍵を有する再生手段でなければ再生不可能となる。従って、複数の情報機器において利用可能な形態を実現するためには、ユーザに提供する暗号鍵を共通化しておくことが必要となる。

【 0 0 2 0 】

しかしながら、コンテンツの暗号鍵を共通化するという事は、正規ライセンスを持たないユーザに暗号処理用の鍵を無秩序に流通させる可能性を高めることになり、正規のライセンスを持たないユーザによるコンテンツの不正利用を防止できなくなるという欠点があり、正規ライセンスを持たないPC、ゲーム機器等での不正利用の排除が困難になる。

【 0 0 2 1 】

さらに、上述のように鍵を共通化した環境においては、例えばあるPC上で作成され、メモリカード、フロッピーディスク等の記憶手段に保存された暗号化されたコンテンツは、別のフロッピーディスクに容易に複製することが可能であり、オリジナルのコンテンツデータではなく複製フロッピーディスクを用いた利用形態が可能となり、ゲーム機器、PC等の情報機器において利用可能なコンテンツデータが多数複製されたり、または改竄されてしまう可能性があった。

【 0 0 2 2 】

【発明が解決しようとする課題】

コンテンツデータの利用を正当な利用者に限定する手法としてデータ暗号化、データ復号化、データ検証、認証処理、署名処理等、各種の暗号処理があるが、これら各種の暗号処理を実行するためには、2つの装置間、すなわち、コンテンツデータを転送する装置間、あるいは認証処理を実行する装置間において、共有する秘密情報、例えばコンテンツデータの暗号化、復号化に適用する鍵情報を共有したり、認証する装置間で認証に使用する認証鍵を共有することが必要となる。

【 0 0 2 3 】

従って例えば、2つの装置のいずれかから、その共有秘密情報である鍵データが漏洩した場合には、その共有鍵情報を用いたコンテンツの暗号化データは、ライセンスを持たない第三者によっても復号可能となり、不正なコンテンツの利用が可能となってしまう。また認証鍵が漏洩した場合にも同様であり、全くライセンスを持たない装置に対する認証が成立してしまい、鍵の漏洩は、システム全体を脅かす結果をもたらす。

【 0 0 2 4 】

本発明は、このような問題点を解決するものである。本発明のデータ処理装置、データ処理システム、およびデータ処理方法は、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の暗号処理を実行するために必要となる個別鍵を記憶部に記憶格納せず、これらの個別鍵を生成するためのマスター鍵を記憶部に格納し、暗号処理部がマスター鍵と、装置またはデータの識別データに基づいて必要な個別鍵を生成することにより、暗号処理におけるセキュリティを高めたデータ処理装置、データ処理システム、およびデータ処理方法を提供する。

【 0 0 2 5 】

【課題を解決するための手段】

本発明の第 1 の側面は、

データ処理装置において、

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理部と、

前記暗号処理に適用する鍵を生成するためのマスター鍵を格納した記憶部とを有し、

前記暗号処理部は、前記暗号処理を実行するに必要な個別鍵を、前記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する構成を有することを特徴とするデータ処理装置にある。

【 0 0 2 6 】

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、記憶媒体または通信媒体を介する転送データに関する暗号処理を行なうデータ処理装置であり、前記記憶部は、前記転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} を格納し、前記暗号処理部は、前記記憶部に格納された配送鍵生成用マスター鍵 MK_{dis} と、前記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行して、前記転送データの配送鍵 K_{dis} を生成する構成を有することを特徴とする。

【 0 0 2 7 】

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置

は、転送データの転送先あるいは転送元となる外部接続装置の認証処理を行なうデータ処理装置であり、前記記憶部は、前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成用マスター鍵 MK_{ake} を格納し、前記暗号処理部は、前記記憶部に格納された認証鍵生成用マスター鍵 MK_{ake} と、前記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、前記外部接続装置の認証鍵 K_{ake} を生成する構成を有することを特徴とする。

【 0 0 2 8 】

さらに、本発明のデータ処理装置の一実施態様において、前記データ処理装置は、データに対する署名処理を実行するデータ処理装置であり、前記記憶部は、前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成用マスター鍵 MK_{dev} を格納し、前記暗号処理部は、前記記憶部に格納された署名鍵生成用マスター鍵 MK_{dev} と、前記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する構成を有することを特徴とする。

【 0 0 2 9 】

さらに、本発明のデータ処理装置の一実施態様において、暗号処理を実行するに必要な個別鍵を、前記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する個別鍵生成処理は、暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、前記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする。

【 0 0 3 0 】

さらに、本発明のデータ処理装置の一実施態様において、前記暗号処理は DES アルゴリズムを適用した暗号処理であることを特徴とする。

【 0 0 3 1 】

さらに、本発明の第 2 の側面は、
複数のデータ処理装置から構成されるデータ処理システムにおいて、
前記複数のデータ処理装置の各々が、データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理に適用する鍵を生成するための共通のマスター鍵を有し、

前記複数のデータ処理装置の各々が、前記マスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて前記暗号処理を実行するに必要な共通の個別鍵を生成する構成を有することを特徴とするデータ処理システムにある。

【 0 0 3 2 】

さらに、本発明のデータ処理システムの一実施態様において、前記複数のデータ処理装置は、コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置によって構成され、コンテンツデータ提供装置およびコンテンツデータ利用装置の双方が、前記コンテンツデータ提供装置およびコンテンツデータ利用装置間における流通コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵を有し、前記コンテンツデータ提供装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、前記コンテンツデータ利用装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行する構成を有することを特徴とする。

【 0 0 3 3 】

さらに、本発明のデータ処理システムの一実施態様において、前記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と前記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、前記コンテンツデータ利用装置は、前記コンテンツデータ提供装置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号可能とした構成を有することを特徴とする。

【 0 0 3 4 】

さらに、本発明のデータ処理システムの一実施態様において、前記複数のデータ処理装置の各々に、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するための同一のコンテンツ鍵生成用マスター鍵を格納し、前記複数のデータ処理装置の1つのデータ処理装置Aにおいて、前記コンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化され記憶媒体に格納されたコンテンツデータを、異なるデータ処理装置Bにおいて、前記同一のコンテンツ鍵生成用マスター鍵と、前記データ処理装置Aの装置識別子とに基づいてコンテンツ鍵を生成し、該生成したコンテンツ鍵に基づいて、前記データ処理装置Aにおいて前記記憶媒体に格納した暗号化コンテンツデータの復号処理を実行する構成としたことを特徴とする。

【0035】

さらに、本発明のデータ処理システムの一実施態様において、前記複数のデータ処理装置は、ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとによって構成され、前記ホストデバイスおよびスレーブデバイスの双方が、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵生成用マスターを有し、前記スレーブデバイスは、前記認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成してスレーブデバイス内メモリに格納し、前記ホストデバイスは、前記認証鍵生成用マスター鍵と、前記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行する構成を有することを特徴とする。

【0036】

さらに、本発明の第3の側面は、

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理を実行するデータ処理方法において、

暗号処理を実行するに必要な個別鍵を、前記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

前記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処

理ステップと、

を有することを特徴とするデータ処理方法にある。

【0037】

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において実行するデータ処理は、記憶媒体または通信媒体を介する転送データに関する暗号処理であり、前記鍵生成ステップは、転送データの暗号処理に適用する配送鍵 K_{dis} を生成する配送鍵生成用マスター鍵 MK_{dis} と、前記転送データの識別データであるデータ識別子とに基づいて暗号処理を実行し、前記転送データの配送鍵 K_{dis} を生成する配送鍵生成ステップであり、前記暗号処理ステップは、前記配送鍵生成ステップにおいて生成した配送鍵 K_{dis} に基づいて転送データの暗号処理を実行するステップであることを特徴とする。

【0038】

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理方法において実行するデータ処理は、転送データの転送先あるいは転送元となる外部接続装置の認証処理であり、前記鍵生成ステップは、前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成用マスター鍵 MK_{ake} と、前記外部接続装置の識別データである外部接続装置識別子とに基づいて暗号処理を実行して、前記外部接続装置の認証鍵 K_{ake} を生成する認証鍵生成ステップであり、前記暗号処理ステップは、前記認証鍵生成ステップにおいて生成した認証鍵 K_{ake} に基づいて外部接続装置の認証処理を実行するステップであることを特徴とする。

【0039】

さらに、本発明のデータ処理方法の一実施態様において、前記データ処理装置において実行するデータ処理は、データに対する署名処理であり、前記鍵生成ステップは、前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成用マスター鍵 MK_{dev} と、前記データ処理装置の識別データであるデータ処理装置識別子とに基づいて暗号処理を実行して、前記データ処理装置のデータ処理装置署名鍵 K_{dev} を生成する署名鍵生成ステップであり、前記暗号処理ステップは、前記署名鍵生成ステップにおいて生成した署名鍵 K_{dev} に基づいてデータに対する署名処理を実行するステップであることを特徴とする。

【0040】

さらに、本発明のデータ処理方法の一実施態様において、前記鍵生成ステップは、暗号処理対象の装置またはデータの識別データの少なくとも一部をメッセージとし、前記マスター鍵を暗号鍵として適用した暗号処理であることを特徴とする。

【0041】

さらに、本発明のデータ処理方法の一実施態様において、前記暗号処理はDESアルゴリズムを適用した暗号処理であることを特徴とする。

【0042】

さらに、本発明の第4の側面は、

コンテンツデータを提供するコンテンツデータ提供装置と、コンテンツデータの利用を行なうコンテンツデータ利用装置とからなるデータ処理システムにおけるデータ処理方法であり、

前記コンテンツデータ提供装置は、コンテンツデータの暗号処理に適用するコンテンツデータ配送鍵を生成するための配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの暗号化処理を実行し、

前記コンテンツデータ利用装置は、前記配送鍵生成用マスター鍵と、提供コンテンツデータの識別子であるコンテンツ識別子とに基づいてコンテンツデータ配送鍵を生成して、該コンテンツデータの復号化処理を実行することを特徴とするデータ処理方法にある。

【0043】

さらに、本発明のデータ処理方法の一実施態様において、前記コンテンツデータ提供装置は、複数の異なるコンテンツデータ配送鍵を生成するための複数の異なる配送鍵生成用マスター鍵を有し、該複数の配送鍵生成用マスター鍵と前記コンテンツ識別子に基づいて複数の異なるコンテンツデータ配送鍵を生成し、該生成した複数の配送鍵による暗号化処理を実行して複数種類の暗号化コンテンツデータを生成し、前記コンテンツデータ利用装置は、前記コンテンツデータ提供装

置の有する複数の異なる配送鍵生成用マスター鍵の少なくとも1つの配送鍵生成用マスター鍵を有し、自己の所有する配送鍵生成用マスター鍵と同じ配送鍵生成用マスター鍵を使用して生成された配送鍵による暗号化コンテンツデータのみを復号することを特徴とする。

【0044】

さらに、本発明の第5の側面は、

複数のデータ処理装置によって構成されるデータ処理システムにおけるデータ処理方法であり、

前記複数のデータ処理装置中の1つのデータ処理装置Aにおいて、コンテンツデータの暗号処理に適用するコンテンツ鍵を生成するためのコンテンツ鍵生成用マスター鍵と、該データ処理装置Aの装置識別子とに基づいて生成されたコンテンツ鍵により暗号化されたコンテンツデータを記憶媒体に格納するステップと、

異なるデータ処理装置Bにおいて、前記データ処理装置Aと同一の前記コンテンツ鍵生成用マスター鍵と前記データ処理装置Aの装置識別子とに基づいて前記コンテンツ鍵と同一のコンテンツ鍵を生成するステップと、

前記データ処理装置Bにおいて生成したコンテンツ鍵により前記記憶媒体に格納したコンテンツデータの復号を行なうステップと、

を有することを特徴とするデータ処理方法にある。

【0045】

さらに、本発明の第6の側面は、

ホストデバイスと、該ホストデバイスの認証処理の対象となるスレーブデバイスとからなるデータ処理システムにおけるデータ処理方法であり、

前記スレーブデバイスは、ホストデバイスとスレーブデバイス間の認証処理に適用する認証鍵を生成するための認証鍵生成用マスター鍵と、該スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成し、生成した認証鍵を該スレーブデバイス内のメモリに格納し、

前記ホストデバイスは、前記認証鍵生成用マスター鍵と、前記スレーブデバイスの識別子であるスレーブデバイス識別子とに基づいて認証鍵を生成して認証処理を実行することを特徴とするデータ処理方法にある。

【0046】

さらに、本発明の第7の側面は、

データ暗号化、データ復号化、データ検証、認証処理、署名処理の少なくともいずれかの暗号処理を実行する暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

暗号処理を実行するに必要な個別鍵を、前記暗号処理に適用する鍵を生成するためのマスター鍵と、暗号処理対象の装置またはデータの識別データに基づいて生成する鍵生成ステップと、

前記鍵生成ステップによって生成した鍵に基づいて暗号処理を実行する暗号処理ステップと、

を含むことを特徴とするプログラム提供媒体にある。

【0047】

本発明に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD、MOなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0048】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的關係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【0049】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0050】

【発明の実施の形態】

以下に本発明の実施の形態を説明する。説明の手順は、以下の項目に従って行なう。

- (1) データ処理装置構成
- (2) コンテンツデータフォーマット
- (3) データ処理装置において適用可能な暗号処理概要
- (4) 記録再生器の格納データ構成
- (5) 記録デバイスの格納データ構成
- (6) 記録再生器、記録デバイス間における相互認証処理
 - (6-1) 相互認証処理の概要
 - (6-2) 相互認証時の鍵ブロックの切り替え
- (7) 記録再生器から記録デバイスへのダウンロード処理
- (8) 記録デバイス格納情報の記録再生器での再生処理
- (9) 相互認証後の鍵交換処理
- (10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理
 - (11) コンテンツプロバイダにおけるチェック値 (ICV) 生成処理態様
 - (12) マスタ鍵に基づく暗号処理鍵生成構成
 - (13) 暗号処理における暗号強度の制御
 - (14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理
- (15) コンテンツ構成および再生(伸長)処理
- (16) セーブデータの生成および記録デバイスへの格納、再生処理
- (17) 不正機器の排除 (リボケーション) 構成
- (18) セキュアチップ構成および製造方法

【0051】

- (1) データ処理装置構成

図2に本発明のデータ処理装置の一実施例に係る全体構成ブロック図を示す。
本発明のデータ処理装置は、記録再生器300と記録デバイス400とを主要構

成要素とする。

【0052】

記録再生器300は、例えばパーソナル・コンピュータ（PC：Personal Computer）、あるいはゲーム機器等によって構成される。記録再生器300は、図2に示すように、記録再生器300における暗号処理時の記録デバイス400との通信制御を含む統括的制御を実行する制御部301、暗号処理全般を司る記録再生器暗号処理部302、記録再生器に接続される記録デバイス400と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ303、DVDなどのメディア500から少なくともデータの読み出しを行う読み取り部304、外部とデータの送受信を行う通信部305を有する。

【0053】

記録再生器300は、制御部301の制御により記録デバイス400に対するコンテンツデータのダウンロード、記録デバイス400からのコンテンツデータ再生を実行する。記録デバイス400は、記録再生器300に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、EEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成される外部メモリ402を有する。

【0054】

記録再生器300は、図2の左端に示す記憶媒体、DVD、CD、FD、HDDに格納されたコンテンツデータを入力可能なインタフェースとしての読み取り部304、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインタフェースとしての通信部305を有し、外部からコンテンツを入力する。

【0055】

記録再生器300は、暗号処理部302を有し、読取部304または通信部305を介して外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいはコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。暗号処理部302は、暗号処理部302全体を制御する制御部30

6、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ307、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部308から構成されている。

【0056】

制御部301は、例えば、記録再生器300に記録デバイス400が装着された際に記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信したり、あるいは、記録再生器暗号処理部302の暗号／復号化部308と記録デバイス暗号処理部401の暗号／復号化部406の間で行われる相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。これらの各処理については、後段で詳細に説明する。

【0057】

暗号処理部302は、前述のように認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、暗号処理制御部306、内部メモリ307、暗号／復号化部308を有する。

【0058】

暗号処理制御部306は、記録再生器300において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、記録再生器300と記録デバイス400との間で実行される認証処理の完了時における認証完了フラグの設定、記録再生器暗号処理部302の暗号／復号化部308において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

【0059】

内部メモリ307は、後段で詳細に説明するが、記録再生器300において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは識別データ等を格納する。

【0060】

暗号／復号化部308は、内部メモリ307に格納された鍵データ等を使用し

て、外部から入力されるコンテンツデータを記録デバイス400にダウンロード処理する際、あるいは記録デバイス400に格納されたコンテンツデータを記録デバイス400から再生、実行する際の認証処理、暗号化処理、復号化処理、さらに所定のチェック値や電子署名の生成・検証、データの検証、乱数の発生などの処理を実行する。

【0061】

ここで、記録再生器暗号処理部302の内部メモリ307は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。この構成については、後段で詳細に説明する。

【0062】

記録再生器300は、これらの暗号処理機能の他に、中央演算処理装置（メインCPU: Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108、AV処理部109、入力インタフェース110、PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112を備えている。

【0063】

中央演算処理装置（メインCPU: Central Processing Unit）106、RAM（Random Access Memory）107、ROM（Read Only Memory）108は、記録再生器300本体の制御系として機能する構成部であり、主として記録再生器暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU: Central Processing Unit）106は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部109へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【0064】

RAM107は、CPU106における各種処理用の主記憶メモリとして使用され、メインCPU106による処理のための作業領域として使用される。ROM108は、メインCPU106で起動されるOS等を立ち上げるための基本プログラム等が格納される。

【0065】

AV処理部109は、具体的には、例えばMPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【0066】

入力インタフェース110は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU106に出力する。メインCPU106は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

【0067】

PIO（パラレルI/Oインタフェース）111、SIO（シリアルI/Oインタフェース）112は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インタフェースとして使用される。

【0068】

また、メインCPU106は、例えば実行中のゲーム等に関する設定データ等をセーブデータとして記録デバイス400に記憶する際の制御も行なう。この処理の際には、記憶データを制御部301に転送し、制御部301は必要に応じて暗号処理部302にセーブデータに関する暗号処理を実行させ、暗号化データを記録デバイス400に格納する。これらの暗号処理については、後段で詳細に説明する。

【0069】

記録デバイス400は、前述したように好ましくは記録再生器300に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバ

イス 4 0 0 は暗号処理部 4 0 1、外部メモリ 4 0 2 を有する。

【0 0 7 0】

記録デバイス暗号処理部 4 0 1 は、記録再生器 3 0 0 からのコンテンツデータのダウンロード、または記録デバイス 4 0 0 から記録再生器 3 0 0 へのコンテンツデータの再生処理時等における記録再生器 3 0 0 と記録デバイス 4 0 0 間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、記録再生器 3 0 0 の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。これらの詳細は図 3 に示す。外部メモリ 4 0 2 は、前述したように、例えば E E P R O M 等のフラッシュメモリからなる不揮発メモリ、ハードディスク、電池つき R A M などによって構成され、暗号化されたコンテンツデータ等を格納する。

【0 0 7 1】

図 3 は、本発明のデータ処理装置がデータ供給を受けるコンテンツ提供手段であるメディア 5 0 0、通信手段 6 0 0 から入力されるデータ構成の概略を示すとともに、これらコンテンツ提供手段 5 0 0、6 0 0 からコンテンツを入力する記録再生器 3 0 0 と、記録デバイス 4 0 0 における暗号処理に関する構成を中心として、その構成を示した図である。

【0 0 7 2】

メディア 5 0 0 は、例えば光ディスクメディア、磁気ディスクメディア、磁気テープメディア、半導体メディア等である。通信手段 6 0 0 は、インターネット通信、ケーブル通信、衛星通信等の、データ通信可能な手段である。

【0 0 7 3】

図 3 において、記録再生器 3 0 0 は、コンテンツ提供手段であるメディア 5 0 0、通信手段 6 0 0 から入力されるデータ、すなわち図 3 に示すような所定のフォーマットに従ったコンテンツを検証し、検証後にコンテンツを記録デバイス 4 0 0 に保存する。

【0 0 7 4】

図 3 のメディア 5 0 0、通信手段 6 0 0 部分に示すようにコンテンツデータは以下のような構成部を有する。

識別情報：コンテンツデータの識別子としての識別情報。

取扱方針：コンテンツデータの構成情報、例えばコンテンツデータを構成するヘッダー部サイズ、コンテンツ部サイズ、フォーマットのバージョン、コンテンツがプログラムかデータか等を示すコンテンツタイプ、さらにコンテンツがダウンロードした機器だけでしか利用できないのか他の機器でも利用できるのか等の利用制限情報等を含む取扱方針。

ブロック情報：コンテンツブロックの数、ブロックサイズ、暗号化の有無を示す暗号化フラグ等から構成されるブロック情報。

鍵データ：上述のブロック情報を暗号化する暗号化鍵、あるいはコンテンツブロックを暗号化するコンテンツ鍵等からなる鍵データ。

コンテンツブロック：実際の再生対象となるプログラムデータ、音楽、画像データ等からなるコンテンツブロック。

を有する。なお、コンテンツデータ詳細については、後段で図 4 以下を用いてさらに詳細に説明する。

【 0 0 7 5 】

コンテンツデータは、コンテンツ鍵（ここでは、これをコンテンツ鍵（Content Key（以下、K c o n とする））と呼ぶ）によって暗号化されて、メディア 5 0 0、通信手段 6 0 0 から記録再生器 3 0 0 に提供される。コンテンツは、記録再生器 3 0 0 を介して記録デバイス 4 0 0 の外部メモリに格納することができる。

【 0 0 7 6 】

例えば、記録デバイス 4 0 0 は、記録デバイス内の内部メモリ 4 0 5 に格納された記録デバイス固有の鍵（ここでは、これを保存鍵（Storage Key（以下、K s t r とする））と呼ぶ）を用いて、コンテンツデータに含まれるコンテンツ、及びコンテンツデータのヘッダ情報として含まれるブロック情報、各種鍵情報、例えばコンテンツ鍵 K c o n などを暗号化して外部メモリ 4 0 2 に記憶する。コンテンツデータの記録再生器 3 0 0 から記録デバイス 4 0 0 へのダウンロード処理、あるいは記録再生器 3 0 0 による記録デバイス 4 0 0 内に格納されたコンテンツデータの再生処理においては、機器間の相互認証処理、コンテンツデータの

暗号化、復号化処理等、所定の手続きが必要となる。これらの処理については、後段で詳細に説明する。

【0077】

記録デバイス400は、図3に示すように暗号処理部401、外部メモリ402を有し、暗号処理部401は、制御部403、通信部404、内部メモリ405、暗号／復号化部406、外部メモリ制御部407を有する。

【0078】

記録デバイス400は、暗号処理全般を司り、外部メモリ402を制御するとともに、記録再生器300からのコマンドを解釈し、処理を実行する記録デバイス暗号処理部401と、コンテンツなどを保持する外部メモリ402からなる。

【0079】

記録デバイス暗号処理部401は、記録デバイス暗号処理部401全体を制御する制御部403、記録再生器300とデータの送受信を行う通信部404、暗号処理用の鍵データなどの情報を保持し、外部から容易に読み出せないように処理が施された内部メモリ405、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部406、外部メモリ402のデータを読み書きする外部メモリ制御部407を有する。

【0080】

制御部403は、記録デバイス400において実行される認証処理、暗号化／復号化処理等の暗号処理全般に係る制御を実行する制御部であり、例えば、記録再生器300と記録デバイス400との間で実行される認証処理の完了時における認証完了フラグの設定、暗号処理部401の暗号／復号化部406において実行される各種処理、例えばダウンロード、あるいは再生コンテンツデータに関するチェック値生成処理の実行命令、各種鍵データの生成処理の実行命令等、暗号処理全般に関する制御を行なう。

【0081】

内部メモリ405は、後段で詳細に説明するが、複数のブロックを持つメモリによって構成されており、記録デバイス400において実行される相互認証処理、チェック値照合処理、暗号化、復号化処理等、各種処理において必要となる鍵

データ、あるいは識別データ等の組を複数格納した構成となっている。

【0082】

記録デバイス暗号処理部401の内部メモリ405は、先に説明した記録再生器暗号処理部302の内部メモリ307と同様、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録デバイス400の暗号処理部401は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされる。なお、記録再生器暗号処理部302は、鍵などの秘密の情報を容易に外部に漏らさないように構成されたソフトウェアであってもよい。

【0083】

暗号／復号化部406は、記録再生器300からのコンテンツデータのダウンロード処理、記録デバイス400の外部メモリ402に格納されたコンテンツデータの再生処理、あるいは、記録再生器300と記録デバイス400間の相互認証処理の際、内部メモリ405に格納された鍵データ等を使用して、データの検証処理、暗号化処理、復号化処理、所定のチェック値や電子署名の生成・検証、乱数の発生などの処理等を実行する。

【0084】

通信部404は、記録再生器300の記録デバイスコントローラ303に接続され、記録再生器300の制御部301、あるいは、記録デバイス403の制御部403の制御に従って、コンテンツデータのダウンロード処理、再生処理、あるいは、相互認証処理の際の記録再生器300と記録デバイス400間の転送データの通信を行なう。

【0085】

(2) コンテンツデータフォーマット

次に、図4乃至図6を用いて、本発明のシステムにおけるメディア500に格納され、またはデータ通信手段600上を流通するデータのデータフォーマットについて説明する。

【0086】

図4に示す構成がコンテンツデータ全体のフォーマットを示す図であり、図5に示す構成がコンテンツデータのヘッダ部の一部を構成する「取扱方針」の詳細を示す図であり、図6に示す構成がコンテンツデータのヘッダ部の一部を構成する「ブロック情報」の詳細を示す図である。

【0087】

なお、ここでは、本発明のシステムにおいて適用されるデータフォーマットの代表的な一例について説明するが、本発明のシステムでは、例えばゲームプログラムに対応したフォーマット、音楽データ等のリアルタイム処理に適したフォーマット等、異なる複数のデータフォーマットが利用可能であり、これらのフォーマットの態様については、後段「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」において、さらに詳しく述べる。

【0088】

図4に示すデータフォーマットにおいて、グレーで示す部分は暗号化されたデータであり、二重枠の部分は改竄チェックデータ、その他の白い部分は暗号化されていない平文のデータである。暗号化部の暗号化鍵は、それぞれの枠の左に示す鍵である。図4に示す例においては、コンテンツ部の各ブロック（コンテンツブロックデータ）に暗号化されたものと暗号化されていないものとが混在している。これらの形態は、コンテンツデータに応じて異なるものであり、データに含まれるすべてのコンテンツブロックデータが暗号化されている構成であってもよい。

【0089】

図4に示すように、データフォーマットは、ヘッダー部とコンテンツ部に分かれており、ヘッダー部は、識別情報（Content ID）、取扱方針（Usage Policy）、チェック値A（Integrity Check Value A（以下、ICV aとする））、ブロック情報鍵（Block Information Table Key（以下、K b i tとする））、コンテンツ鍵K c o n、ブロック情報（Block Information Table（以下、B I Tとする））、チェック値B（ICV b）、総チェック値（ICV t）により構成

されており、コンテンツ部は、複数のコンテンツブロック（例えば暗号化されたコンテンツと、暗号化されていないコンテンツ）から構成されている。

【0090】

ここで、識別情報は、コンテンツを識別するための個別の識別子（Content ID）を示している。取扱方針は、図5にその詳細を示すように、ヘッダ一部分のサイズを示すヘッダサイズ（Header Length）、コンテンツ部分のサイズを示すコンテンツサイズ（Content Length）、フォーマットのバージョン情報を示すフォーマットバージョン（Format Version）、フォーマットの種類を示すフォーマットタイプ（Format Type）、コンテンツ部に保存されているコンテンツがプログラムなのか、データなのか等コンテンツの種類を示すコンテンツタイプ（Content Type）、コンテンツタイプがプログラムである場合の起動優先順位を示す起動優先順位情報（Operation Priority）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器だけでしか利用できないのか、他の同様な機器でも利用できるのかを示す利用制限情報（Localization Field）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に複製できるのか否かを示す複製制限情報（Copy Permission）、このフォーマットに従ってダウンロードされたコンテンツが、ダウンロードした機器から他の同様な機器に移動できるのか否かを示す移動制限情報（Move Permission）、コンテンツ部内のコンテンツブロックを暗号するのに使用したアルゴリズムを示す暗号アルゴリズム（Encryption Algorithm）、コンテンツ部内のコンテンツを暗号化するのに使用したアルゴリズムの使用方法を示す暗号化モード（Encryption Mode）、チェック値の生成方法を示す検証方法（Integrity Check Method）から構成されている。

【0091】

なお、上述した取扱方針に記録するデータ項目は、1つの例であり、対応するコンテンツデータの態様に応じて様々な取扱方針情報を記録することが可能である。例えば後段の「（17）不正機器の排除（リボケーション）構成」で詳しく述べるが、不正な記録再生器の識別子をデータとして記録して、利用開始時の照合によって不正機器によるコンテンツ利用を排除するように構成することも可能

である。

【0092】

チェック値A, I C V a は、識別情報、取扱方針の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値、すなわち部分チェック値として機能する。データブロック情報鍵K b i t は、ブロック情報を暗号化するのに用いられ、コンテンツ鍵K c o n は、コンテンツブロックを暗号化するのに用いられる。なお、ブロック情報鍵K b i t 及びコンテンツ鍵K c o n は、メディア500上および通信手段600上では後述する配送鍵(Distribution Key (以下、K d i s とする))で暗号化されている。

【0093】

ブロック情報の詳細を図6に示す。なお、図6のブロック情報は、図4から理解されるようにすべてブロック情報鍵K b i t によって暗号化されているデータである。ブロック情報は、図6に示すように、コンテンツブロックの数を示すコンテンツブロック数(Block Number)とN個のコンテンツブロック情報から構成されている。コンテンツブロック情報は、ブロックサイズ(Block Length)、暗号化されているか否かを示す暗号化フラグ(Encryption Flag)、チェック値を計算する必要があるか否かを示す検証対象フラグ(I C V Flag)、コンテンツチェック値(I C V i)から構成されている。

【0094】

コンテンツチェック値は、各コンテンツブロックの改竄を検証するために用いられるチェック値である。コンテンツチェック値の生成手法の具体例については、後段の「(10)複数のデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理」の欄で説明する。なお、ブロック情報を暗号化しているブロック情報鍵K b i t は、さらに、配送鍵K d i s によって暗号化されている。

【0095】

図4のデータフォーマットの説明を続ける。チェック値B, I C V b は、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値である。コンテンツデータ全体ではなく部分データのチェック値

、すなわち部分チェック値として機能する。総チェック値 ICV_t は、 ICV_a 、 ICV_b 、各コンテンツブロックのチェック値 ICV_i （設定されている場合）、これらの部分チェック値、あるいはそのチェック対象となるデータ全ての改竄を検証するためのチェック値である。

【0096】

なお、図6においては、ブロックサイズ、暗号化フラグ、検証対象フラグを自由に設定できるようにしているが、ある程度ルールを決めた構成としてもよい。例えば、暗号文領域と平文領域を固定サイズ繰り返しにしたり、全コンテンツデータを暗号化したりし、ブロック情報 BIT を圧縮してもよい。また、コンテンツ鍵 K_{con} をコンテンツブロック毎に異なるようにするため、コンテンツ鍵 K_{con} をヘッダー部分ではなく、コンテンツブロックに含ませるようにしてもよい。コンテンツデータフォーマットの例については、「(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理」の項目において、さらに詳細に説明する。

【0097】

(3) 本発明のデータ処理装置において適用可能な暗号処理概要

次に、本発明のデータ処理装置において適用され得る各種暗号処理の態様について説明する。なお、本項目「(3) 本発明のデータ処理装置において適用可能な暗号処理の概要」に示す暗号処理に関する説明は、後段で具体的に説明する本発明のデータ処理装置における各種処理、例えば a. 記録再生器と記録デバイス間での認証処理。b. コンテンツの記録デバイスに対するダウンロード処理。c. 記録デバイスに格納したコンテンツの再生処理等の処理において実行される処理の基礎となる暗号処理の態様について、その概要を説明するものである。記録再生器 300 と記録デバイス 400 における具体的処理については、本明細書の項目 (4) 以下において、各処理毎に詳細に説明する。

【0098】

以下、データ処理装置において適用可能な暗号処理の概要について、

(3-1) 共通鍵暗号方式によるメッセージ認証

(3-2) 公開鍵暗号方式による電子署名

(3-3) 公開鍵暗号方式による電子署名の検証

(3-4) 共通鍵暗号方式による相互認証

(3-5) 公開鍵証明書

(3-6) 公開鍵暗号方式による相互認証

(3-7) 楕円曲線暗号を用いた暗号化処理

(3-8) 楕円曲線暗号を用いた復号化処理

(3-9) 乱数生成処理

の順に説明する。

【0099】

(3-1) 共通鍵暗号方式によるメッセージ認証

まず、共通鍵暗号方式を用いた改竄検出データの生成処理について説明する。

改竄検出データは、改竄の検出を行ないたいデータに付け、改竄のチェックおよび作成者認証をするためのデータである。

【0100】

例えば、図4で説明したデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値等が、この改竄検出データとして生成される。

【0101】

ここでは、電子署名データの生成処理方法の例の1つとして共通鍵暗号方式におけるDESを用いた例を説明する。なお、本発明においては、DES以外にも、同様の共通鍵暗号方式における処理として例えばFEAL (Fast Encipherment Algorithm: NTT)、AES (Advanced Encryption Standard: 米国次期標準暗号) 等を用いることも可能である。

【0102】

一般的なDESを用いた電子署名の生成方法を図7を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを8バイト単位に分割する(以下、分割されたメッセージをM1、M2、・・・、MNとする)。そして、初期値 (Initial Value (以下、IVとする)) とM1を排他的論理和する(その結果をI1とする)。次に、I1をDES暗号化部に入れ、鍵(以

下、 K_1 とする)を用いて暗号化する(出力を E_1 とする)。続けて、 E_1 および M_2 を排他的論理和し、その出力 I_2 をDES暗号化部へ入れ、鍵 K_1 を用いて暗号化する(出力 E_2)。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきた E_N が電子署名になる。この値は一般にはメッセージ認証符号(MAC(Message Authentication Code))と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをCBC(Cipher Block Chaining)モードと呼ぶ。

【0103】

なお、図7のような生成例において出力されるMAC値が、図4で示すデータ構造中の二重枠部分の各チェック値A、B、総チェック値、および図6に示すブロック情報中の各ブロックに格納されたコンテンツチェック値 $ICV_1 \sim ICV_N$ として使用可能である。このMAC値の検証時には、検証者が生成時と同様の方法でMAC値を生成し、同一の値が得られた場合、検証成功とする。

【0104】

なお、図7に示す例では初期値IVを、初めの8バイトメッセージ M_1 に排他的論理和したが、初期値 $IV = 0$ として、初期値を排他的論理和しない構成とすることも可能である。

【0105】

図7に示すMAC値生成方法に対して、さらにセキュリティを向上させたMAC値生成方法を示す処理構成図を図8に示す。図8は、図7のシングルDESに代えてトリプルDES(Triple DES)を用いてMAC値の生成を実行する例を示したものである。

【0106】

図8に示す各トリプルDES(Triple DES)構成部の詳細構成例を図9に示す。図9(a)、(b)に示すようにトリプルDES(Triple DES)としての構成には2つの異なる態様がある。図9(a)は、2つの暗号鍵を用いた例を示すものであり、鍵1による暗号化処理、鍵2による復号化処理、さらに鍵1による暗号化処理の順に処理を行う。鍵は、 K_1 、 K_2 、 K_1 の順に2種類用いる。図9(b)は3つの暗号鍵を用いた例を示すものであり、鍵1による暗号化

処理、鍵 2 による暗号化処理、さらに鍵 3 による暗号化処理の順に処理を行い 3 回とも暗号化処理を行う。鍵は、K 1、K 2、K 3 の順に 3 種類の鍵を用いる。このように複数の処理を連続させる構成とすることで、シングル D E S に比較してセキュリティ強度を向上させている。しかしながら、このトリプル D E S (Triple D E S) 構成は、処理時間がシングル D E S のおよそ 3 倍かかるという欠点を有する。

【0107】

図 8 および図 9 で説明したトリプル D E S 構成を改良した M A C 値生成構成例を図 1 0 に示す。図 1 0 においては、署名対象となるメッセージ列の初めから途中までの各メッセージに対する暗号化処理は全てシングル D E S による処理とし、最後のメッセージに対する暗号化処理のみを図 9 (a) に示すトリプル D E S (Triple D E S) 構成としたものである。

【0108】

図 1 0 に示すこのような構成とすることで、メッセージの M A C 値の生成処理時間は、シングル D E S による M A C 値生成処理に要する時間とほぼ同程度に短縮され、かつセキュリティはシングル D E S による M A C 値よりも高めることが可能となる。なお、最終メッセージに対するトリプル D E S 構成は、図 9 (b) の構成とすることも可能である。

【0109】

(3-2) 公開鍵暗号方式による電子署名

以上は、暗号化方式として共通鍵暗号化方式を適用した場合の電子署名データの生成方法であるが、次に、暗号化方式として公開鍵暗号方式を用いた電子署名の生成方法を図 1 1 を用いて説明する。図 1 1 に示す処理は、E C - D S A ((Elliptic Curve Digital Signature Algorithm) 、IEEE P1363/D3) を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号 (Elliptic Curve Cryptography (以下、ECC と呼ぶ)) を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えば R S A 暗号 ((Rivest, Shamir, Adleman) など (ANSI X9.31)) を用いることも可能である。

【0110】

図11の各ステップについて説明する。ステップS1において、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップS2において、メッセージ M のハッシュ値を計算し、 $f = \text{Hash}(M)$ とする。

【0111】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、図7他で説明したと同様のDES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0112】

続けて、ステップS3で、乱数 u （ $0 < u < r$ ）を生成し、ステップS4でベースポイントを u 倍した座標 $V(X_v, Y_v)$ を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0113】

【数1】

$P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、

$P \neq Q$ の時（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P=Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

【0114】

これらを用いて点Gの u 倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。 G 、 $2 \times G$ 、 $4 \times G \cdots$ を計算し、 u を2進数展開して1が立っているところに対応する $2^i \times G$ （ G を i 回2倍算した値）を加算する（ i は u のLSBから数えた時のビット位置））。

【0115】

ステップS5で、 $c = Xv \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + cKs) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0116】

ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱数を生成し直す。同様に、ステップS8で d が0であった場合も、ステップS3に戻って乱数を生成し直す。

【0117】

(3-3) 公開鍵暗号方式による電子署名の検証

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図12を用いて説明する。ステップS11で、 M をメッセージ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $Ks \times G$ を公開鍵（ $0 < Ks < r$ ）とする。ステップS12で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS13で、メッセージ M のハッシュ値を計算し、 $f = Hash(M)$ とする。次に、ステップS14で $h = 1/d \bmod r$ を計算し、ステップS15で $h1 = fh \bmod r$ 、 $h2 = ch \bmod r$ を計算する。

【0118】

ステップS16において、既に計算した $h1$ および $h2$ を用い、点 $P = (Xp, Yp) = h1 \times G + h2 \cdot Ks \times G$ を計算する。電子署名検証者は、公開鍵 G

および $K_s \times G$ を知っているのので、図 11 のステップ S4 と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップ S17 で点 P が無限遠点かどうか判定し、無限遠点でなければステップ S18 に進む（実際には、無限遠点の判定はステップ S16 でできてしまう。つまり、 $P = (X, Y)$ 、 $Q = (X, -Y)$ の加算を行うと、 λ が計算できず、 $P + Q$ が無限遠点であることが判明している）。ステップ S18 で $X_p \bmod r$ を計算し、電子署名データ c と比較する。最後に、この値が一致していた場合、ステップ S19 に進み、電子署名が正しいと判定する。

【0119】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0120】

ステップ S12 において、電子署名データ c または d が、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップ S20 に進む。また、ステップ S17 において、点 P が無限遠点であった場合もステップ S20 に進む。さらにまた、ステップ S18 において、 $X_p \bmod r$ の値が、電子署名データ c と一致していなかった場合にもステップ S20 に進む。

【0121】

ステップ S20 において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【0122】

(3-4) 共通鍵暗号方式による相互認証

次に、共通鍵暗号方式を用いた相互認証方法を、図 13 を用いて説明する。図 13 において、共通鍵暗号方式として DES を用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図 13 において、まず、B が 64 ビットの乱数 R_b を生成し、 R_b および自己の ID である $ID(b)$ を A に送信する。これを受信した A は、新たに 64 ビットの乱数 R_a を生成し、 R_a 、 R_b 、 $ID(b)$ の順に、DES の CBC モードで鍵 K_{ab} を用いてデータを暗号化し、B

に返送する。図 7 に示す DES の CBC モード処理構成によれば、 R_a が M_1 、 R_b が M_2 、 $ID(b)$ が M_3 に相当し、初期値： $IV=0$ としたときの出力 E_1 、 E_2 、 E_3 が暗号文となる。

【0123】

これを受信した B は、受信データを鍵 $K_{a,b}$ で復号化する。受信データの復号化方法は、まず、暗号文 E_1 を鍵 $K_{a,b}$ で復号化し、乱数 R_a を得る。次に、暗号文 E_2 を鍵 $K_{a,b}$ で復号化し、その結果と E_1 を排他的論理和し、 R_b を得る。最後に、暗号文 E_3 を鍵 $K_{a,b}$ で復号化し、その結果と E_2 を排他的論理和し、 $ID(b)$ を得る。こうして得られた R_a 、 R_b 、 $ID(b)$ の内、 R_b および $ID(b)$ が、B が送信したものと一致するか検証する。この検証に通った場合、B は A を正当なものとして認証する。

【0124】

次に B は、認証後に使用するセッション鍵 (Session Key (以下、 K_{ses} とする)) を生成する (生成方法は、乱数を用いる)。そして、 R_b 、 R_a 、 K_{ses} の順に、DES の CBC モードで鍵 $K_{a,b}$ を用いて暗号化し、A に返送する。

【0125】

これを受信した A は、受信データを鍵 $K_{a,b}$ で復号化する。受信データの復号化方法は、B の復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R_b 、 R_a 、 K_{ses} の内、 R_b および R_a が、A が送信したものと一致するか検証する。この検証に通った場合、A は B を正当なものとして認証する。互いに相手を認証した後には、セッション鍵 K_{ses} は、認証後の秘密通信のための共通鍵として利用される。

【0126】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0127】

(3-5) 公開鍵証明書

次に、公開鍵証明書について図 14 を用いて説明する。公開鍵証明書は、公開

鍵暗号方式における認証局（CA：Certificate Authority）が発行する証明書であり、ユーザが自己のID、公開鍵等を認証局に提出することにより、認証局側が認証局のIDや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。

【0128】

図14に示す公開鍵証明書は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザID）、証明書利用者の公開鍵並びに電子署名を含む。

【0129】

電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。この電子署名の生成には、例えば図11で説明した処理フローが適用される。

【0130】

認証局は、図14に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0131】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図12で説明したのでその詳細は省略する。

【0132】

(3-6) 公開鍵暗号方式による相互認証

次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図15を用いて説明する。図15において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図15において、まずBが、64ビットの乱数 R_b を生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数 R_a および標数 p より小さい乱数 A_k を生成する。そして、ベースポイント G を A_k 倍した点 $A_v = A_k \times G$ を求め、 R_a 、 R_b 、 A_v (X座標とY座標) に対する電子署名 $A.Sig$ を生成し、Aの公開鍵証明書とともにBに返送する。ここで、 R_a および R_b はそれぞれ64ビット、 A_v のX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図11で説明したので、その詳細は省略する。また、公開鍵証明書も図14で説明したので、その詳細は省略する。

【0133】

Aの公開鍵証明書、 R_a 、 R_b 、 A_v 、電子署名 $A.Sig$ を受信したBは、Aが送信してきた R_b が、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。公開鍵証明書の検証については、図14を用いて説明したので、その詳細は省略する。そして、取り出したAの公開鍵を用い電子署名 $A.Sig$ を検証する。電子署名の検証方法は図12で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0134】

次に、Bは、標数 p より小さい乱数 B_k を生成する。そして、ベースポイント G を B_k 倍した点 $B_v = B_k \times G$ を求め、 R_b 、 R_a 、 B_v (X座標とY座標) に対する電子署名 $B.Sig$ を生成し、Bの公開鍵証明書とともにAに返送する。

【0135】

Bの公開鍵証明書、 R_b 、 R_a 、 A_v 、電子署名 $B.Sig$ を受信したAは、

B が送信してきた R_a が、A が生成したものと一致するか検証する。その結果、一致していた場合には、B の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、B の公開鍵を取り出す。そして、取り出した B の公開鍵を用い電子署名 B_{Sig} を検証する。電子署名の検証に成功した後、A は B を正当なものとして認証する。

【0136】

両者が認証に成功した場合には、B は $B_k \times A_v$ (B_k は乱数だが、 A_v は楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要) を計算し、A は $A_k \times B_v$ を計算し、これら点の X 座標の下位 64 ビットをセッション鍵として以降の通信に使用する (共通鍵暗号を 64 ビット鍵長の共通鍵暗号とした場合)。もちろん、Y 座標からセッション鍵を生成してもよいし、下位 64 ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0137】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0138】

(3-7) 楕円曲線暗号を用いた暗号化処理

次に、楕円曲線暗号を用いた暗号化について、図 16 を用いて説明する。ステップ S21 において、 M_x 、 M_y をメッセージ、 p を標数、 a 、 b を楕円曲線の係数 (楕円曲線: $y^2 = x^3 + ax + b$)、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $K_s \times G$ を公開鍵 ($0 < K_s < r$) とする。ステップ S22 で乱数 u を $0 < u < r$ になるように生成し、ステップ S23 で公開鍵 $K_s \times G$ を u 倍した座標 V を計算する。なお、楕円曲線上のスカラー倍は図 11 のステップ S4 で説明したので、詳細は省略する。ステップ S24 で、 V の X 座標を M_x 倍して p で剰余を求め X_0 とし、ステップ S25 で V の Y 座標を M_y 倍して p で剰余を求め Y_0 とする。なお、メッセージの長さが p のビット数より少ない場合、 M_y は乱数を使い、復号化部では M_y を破棄するようにする。ステップ S26 において、 $u \times G$ を計算し、ステップ S27 で暗号文 $u \times G$ 、 (X_0, Y_0) を得る。

【0139】

(3-8) 楕円曲線暗号を用いた復号化処理

次に、楕円曲線暗号を用いた復号化について、図17を用いて説明する。ステップS31において、 $u \times G$ 、 (X_0, Y_0) を暗号文データ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 K_s を秘密鍵（ $0 < K_s < r$ ）とする。ステップS32において、暗号データ $u \times G$ を秘密鍵 K_s 倍し、座標 $V(X_v, Y_v)$ を求める。ステップS33では、暗号データの内、 (X_0, Y_0) の X 座標を取り出し、 $X_1 = X_0 / X_v \bmod p$ を計算し、ステップS34においては、 Y 座標を取り出し、 $Y_1 = Y_0 / Y_v \bmod p$ を計算する。そして、ステップS35で X_1 を M_x とし、 Y_1 を M_y としてメッセージを取り出す。この時、 M_y をメッセージにしていなかった場合、 Y_1 は破棄する。

【0140】

このように、秘密鍵を K_s 、公開鍵を G 、 $K_s \times G$ とすることで、暗号化に使用する鍵と復号化に使用する鍵を、異なる鍵とすることができる。

【0141】

また、公開鍵暗号の他の例としてはRSA暗号が知られているが、詳しい説明は省略する（PKCS #1 Version2に詳細が記述されている）。

【0142】

(3-9) 乱数生成処理

次に、乱数の生成方法について説明する。乱数の生成方法としては、熱雑音を増幅し、そのA/D出力から生成する真性乱数生成法や、M系列等の線形回路を複数組み合わせ生成する疑似乱数生成法等が知られている。また、DES等の共通鍵暗号を用いて生成する方法も知られている。本例では、DESを用いた疑似乱数生成方法について説明する（ANSI X9.17ベース）。

【0143】

まず、時間等のデータから得られた64ビット（これ以下のビット数の場合、上位ビットを0とする）の値を D 、Triple-DESに使われる鍵情報を K_r 、乱数発生用の種（Seed）を S とする。このとき、乱数 R は以下のように

計算される。

【0144】

【数2】

$$I = \text{Triple-DES}(K_r, D) \dots\dots\dots (2-1)$$

$$R = \text{Triple-DES}(K_r, S^{\wedge} I) \dots\dots\dots (2-2)$$

$$S = \text{Triple-DES}(K_r, R^{\wedge} I) \dots\dots\dots (2-3)$$

【0145】

ここで、 $\text{Triple-DES}()$ は、第1引数を暗号鍵情報として、第2引数の値を Triple-DES で暗号化する関数とし、演算 $^{\wedge}$ は64ビット単位の排他的論理和、最終的にでてきた値 S は、新規の Seed （種）として更新されていくものとする。

【0146】

以下、連続して乱数を生成する場合には、(2-2)式、(2-3)式を繰り返すものとする。

【0147】

以上、本発明のデータ処理装置において適用可能な暗号処理に関する各種処理態様について説明した。次に、本発明のデータ処理装置において実行される具体的な処理について、詳細に説明する。

【0148】

(4) 記録再生器の格納データ構成

図18は、図3で示す記録再生器300での記録再生器暗号処理部302に構成された内部メモリ307のデータ保持内容を説明する図である。

【0149】

図18に示すように、内部メモリ307には、以下の鍵、データが格納されている。

MKake : 記録再生器300と記録デバイス400（図3参照）との間で実行される相互認証処理に必要な認証鍵（Authentication and Key Exchange Key（以下、 Kake とする））を生成するための記録デバイス認証鍵用マスター鍵

I V a k e : 記録デバイス認証鍵用初期値。

M K d i s : 配送鍵 K d i s を生成するための配送鍵用マスター鍵。

I V d i s : 配送鍵生成用初期値。

K i c v a : チェック値 I C V a を生成するための鍵であるチェック値 A 生成鍵。

K i c v b : チェック値 I C V b を生成するための鍵であるチェック値 B 生成鍵。

K i c v c : 各コンテンツブロックのチェック値 I C V i (i = 1 ~ N) を生成するための鍵であるコンテンツチェック値生成鍵。

K i c v t : 総チェック値 I C V t を生成するための鍵である総チェック値生成鍵。

K s y s : 配信システムに共通の署名または I C V をつけるために使用するシステム署名鍵。

K d e v : 記録再生器毎に異なり、記録再生器が署名または I C V をつけるために使用する記録再生器固有の記録再生器署名鍵。

I V m e m : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。記録デバイスと共通。

これらの鍵、データが記録再生器暗号処理部 3 0 2 に構成された内部メモリ 3 0 7 に格納されている。

【0150】

(5) 記録デバイスの格納データ構成

図 1 9 は、記録デバイス上でのデータ保持状況を示す図である。図 1 9 において、内部メモリ 4 0 5 は、複数のブロック（本例では N ブロック）に分割されており、それぞれのブロック中に、以下の鍵、データが格納されている。

I D m e m : 記録デバイス識別情報、記録デバイス固有の識別情報。

K a k e : 認証鍵、記録再生器 3 0 0 との相互認証時に用いる認証鍵。

I V m e m : 初期値、相互認証処理等の際の暗号処理に用いられる初期値。

K s t r : 保存鍵、ブロック情報鍵他のコンテンツデータの暗号鍵。

K r : 乱数生成鍵、

S : 種

これらのデータを個別のブロックに各々保持している。外部メモリ402は複数（本例ではM個）のコンテンツデータを保持しており、それぞれ図4で説明したデータを、例えば図26、または図27のように保持している。図26、図27の構成の差異については後段で説明する。

【0151】

(6) 記録再生器、記録デバイス間における相互認証処理

(6-1) 相互認証処理の概要

図20は、記録再生器300と記録デバイス400との認証手順を示す流れ図である。ステップS41において、利用者が記録デバイス400を記録再生器300に挿入する。ただし非接触で通信できる記録デバイスを使用する場合には、挿入する必要はない。

【0152】

記録再生器300に記録デバイス400をセットすると、図3に示す記録再生器300内の記録デバイス検知手段（図示せず）が、制御部301に記録デバイス400の装着を通知する。次に、ステップS42において、記録再生器300の制御部301は、記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信する。これを受信した記録デバイス400は、記録デバイス暗号処理部401の制御部403において、通信部404を介して命令を受信し、認証完了フラグがセットされていればクリアする。すなわち未認証状態に設定する。

【0153】

次に、ステップS43において、記録再生器300の制御部301は、記録再生器暗号処理部302に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器300に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス400との認証処理、およびデータ送受信が可能となる。

【0154】

初期化命令を受信した記録再生器300の記録再生器暗号処理部302は、記

録再生器暗号処理部302の制御部306において、記録デバイス挿入口番号に対応する認証完了フラグがセットされていればクリアする。すなわち未認証状態に設定する。

【0155】

次に、ステップS44において、記録再生器300の制御部301は、記録デバイス400の記録デバイス暗号処理部401が使う鍵ブロック番号を指定する。なお、鍵ブロック番号の詳細に関しては後述する。ステップS45において、記録再生器300の制御部301は、記録デバイス400の内部メモリ405の指定された鍵ブロックに格納された記録デバイス識別情報IDmemを読み出す。ステップS46において、記録再生器300の制御部301は、記録再生器暗号処理部302に記録デバイス識別情報IDmemを送信し、記録デバイス識別情報IDmemに基づく認証鍵Kakeを生成させる。認証鍵Kakeの生成方法としては、例えば次のように生成する。

【0156】

【数3】

$$Kake = DES(MKake, IDmem \wedge IVake)$$

【0157】

ここで、MKakeは、記録再生器300と記録デバイス400（図3参照）との間で実行される相互認証処理に必要な認証鍵Kakeを生成するための記録デバイス認証鍵用マスター鍵であり、これは、前述したように記録再生器300の内部メモリ307に格納されている鍵である。またIDmemは、記録デバイス400に固有の記録デバイス識別情報である。さらにIVakeは、記録デバイス認証鍵用初期値である。また、上記式において、DES（）は、第1引数を暗号鍵として、第2引数の値をDESで暗号化する関数であり、演算 \wedge は64ビット単位の排他的論理和を示す。

【0158】

例えば図7、図8に示すDES構成を適用する場合には、図7、8に示されるメッセージMを記録デバイス識別情報：IDmemとし、鍵K1をデバイス認証

鍵用マスター鍵：MKakeとし、初期値IVを：IVakeとして得られる出力が認証鍵Kakeとなる。

【0159】

次に、ステップS47で相互認証およびセッション鍵Ksesの生成処理を行う。相互認証は、記録再生器暗号処理部302の暗号／復号化部308と記録デバイス暗号処理部401の暗号／復号化部406の間で行われ、その仲介を記録再生器300の制御部301が行っている。

【0160】

相互認証処理は、例えば前述の図13で説明した処理にしたがって実行することができる。図13に示す構成において、A、Bがそれぞれ記録再生器300と記録デバイス400に対応する。まず、記録再生器300の記録再生器暗号処理部302が乱数Rbを生成し、乱数Rbおよび自己のIDである記録再生器識別情報IDdevを記録デバイス400の記録デバイス暗号処理部401に送信する。なお、記録再生器識別情報IDdevは、記録再生器300内に構成された記憶部に記憶された再生器固有の識別子である。記録再生器暗号処理部302の内部メモリ中に記録再生器識別情報IDdevを記録する構成としてもよい。

【0161】

乱数Rbおよび記録再生器識別情報IDdevを受信した記録デバイス400の記録デバイス暗号処理部401は、新たに64ビットの乱数Raを生成し、Ra、Rb、と記録再生器識別情報IDdevの順に、DESのCBCモードで認証鍵Kakeを用いてデータを暗号化し、記録再生器300の記録再生器暗号処理部302に返送する。例えば、図7に示すDESのCBCモード処理構成によれば、RaがM1、RbがM2、IDdevがM3に相当し、初期値：IV=IVmemとしたときの出力E1、E2、E3が暗号文となる。

【0162】

暗号文E1、E2、E3を受信した記録再生器300の記録再生器暗号処理部302は、受信データを認証鍵Kakeで復号化する。受信データの復号化方法は、まず、暗号文E1を認証鍵Kakeで復号化し、その結果とIVmemとを排他的論理和し、乱数Raを得る。次に、暗号文E2を認証鍵Kakeで復号化

し、その結果と E 1 を排他的論理和し、R b を得る。最後に、暗号文 E 3 を認証鍵 K a k e で復号化し、その結果と E 2 を排他的論理和し、記録再生器識別情報 I D d e v を得る。こうして得られた R a、R b、記録再生器識別情報 I D d e v の内、R b および記録再生器識別情報 I D d e v が、記録再生器 3 0 0 が送信したものと一致するか検証する。この検証に通った場合、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は記録デバイス 4 0 0 を正当なものとして認証する。

【 0 1 6 3 】

次に、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は、認証後に使用するセッション鍵 (Session Key (以下、K s e s とする)) を生成する (生成方法は、乱数を用いる)。そして、R b、R a、K s e s の順に、D E S の C B C モードで鍵 K a k e、初期値 I V m e m を用いて暗号化し、記録デバイス 4 0 0 の記録デバイス暗号処理部 4 0 1 に返送する。

【 0 1 6 4 】

これを受信した記録デバイス 4 0 0 の記録デバイス暗号処理部 4 0 1 は、受信データを鍵 K a k e で復号化する。受信データの復号化方法は、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 における復号化処理と同様であるので、ここでは詳細を省略する。こうして得られた R b、R a、K s e s の内、R b および R a が、記録デバイス 4 0 0 が送信したものと一致するか検証する。この検証に通った場合、記録デバイス 4 0 0 の記録デバイス暗号処理部 4 0 1 は記録再生器 3 0 0 を正当なものとして認証する。互いに相手を認証した後には、セッション鍵 K s e s は、認証後の秘密通信のための共通鍵として利用される。

【 0 1 6 5 】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものととして処理を中断する。

【 0 1 6 6 】

相互認証に成功した場合には、ステップ S 4 8 からステップ S 4 9 に進み、セッション鍵 K s e s を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 で保持するとともに、相互認証が終了したことを示す認証完了フラグをセットする。また、相互認証に失敗した場合には、ステップ S 5 0 に進み、認証処理過程で生成さ

れたセッション鍵 K_{ses} を破棄するとともに、認証完了フラグをクリアする。
なお、すでにクリアされている場合には必ずしもクリア処理は必要ではない。

【0167】

なお、記録デバイス400が記録デバイス挿入口から取り除かれた場合には、記録再生器300内の記録デバイス検知手段が、記録再生器300の制御部301に記録デバイス400が取り除かれたことを通知し、これを受けた記録再生器300の制御部301は、記録再生器300の記録再生器暗号処理部302に対し記録デバイス挿入口番号に対応する認証完了フラグをクリアするように命令し、これを受けた記録再生器300の記録再生器暗号処理部302は、記録デバイス挿入口番号に対応する認証完了フラグをクリアする。

【0168】

なお、ここでは相互認証処理を図13に示す手続きにしたがって実行する例について説明したが、上述した認証処理例に限らず、例えば先に説明した図15の相互認証手続きに従った処理を実行してもよい。また、図13に示す手続きにおいて、図13のAを記録再生器300とし、Bを記録デバイス400とし、B：記録デバイス400がA：記録再生器300に最初に送付するIDを記録デバイス中の鍵ブロック中の記録デバイス識別情報として相互認証処理を行なってもよい。本発明において実行される認証処理手続きは、様々な処理が適用可能であり、上述の認証処理に限定されるものではない。

【0169】

(6-2) 相互認証時の鍵ブロックの切り替え

本発明のデータ処理装置における相互認証処理における1つの特徴は、記録デバイス400側に複数の鍵ブロック (ex. N個の鍵ブロック) を構成して、記録再生器300が1つの鍵ブロックを指定 (図20の処理フローにおけるステップS44) して認証処理を実行する点である。先に図19において説明したように、記録デバイス400の暗号処理部401に構成された内部メモリ405には複数の鍵ブロックが形成されており、それぞれが異なる鍵データ、ID情報等各種データを格納している。図20で説明した記録再生器300と記録デバイス400間で実行される相互認証処理は、図19の記録デバイス400の複数の鍵ブ

ロックの1つの鍵ブロックに対して実行される。

【0170】

従来、記憶媒体とその再生機器間における相互認証処理を実行する構成では、相互認証に用いる鍵：認証鍵は共通なものが使用されるのが一般的であった。従って、例えば製品仕向け先（国別）ごと、あるいは製品ごとに認証鍵を変更しようとする、記録再生器側と、記録デバイス側の認証処理に必要となる鍵データを双方の機器において変更することが必要となる。従って例えば新たに発売された記録再生器に格納された認証処理に必要となる鍵データは、先に販売された記録デバイスに格納された認証処理に必要となる鍵データに対応せず、新たな記録再生器は、古いバージョンの記録デバイスへのアクセスができなくなってしまう事態が発生する。逆に新しいバージョンの記録デバイスと古いバージョンの記録再生器との関係においても同様の事態が発生する。

【0171】

本発明のデータ処理装置においては、図19に示すように予め記録デバイス400に複数の異なる鍵セットとしての鍵ブロックが格納されている。記録再生器は例えば製品仕向け先（国別）ごと、あるいは製品、機種、バージョン、アプリケーションごとに、認証処理に適用すべき鍵ブロック、すなわち指定鍵ブロックが設定される。この設定情報は、記録再生器のメモリ部、例えば、図3における内部メモリ307、あるいは、記録再生器300の有するその他の記憶素子内に格納され、認証処理時に図3の制御部301によってアクセスされ設定情報にしたがった鍵ブロック指定が行われる。

【0172】

記録再生器300の内部メモリ307の記録デバイス認証鍵用マスター鍵Master Keyは、それぞれの指定鍵ブロックの設定に従って設定された認証鍵用マスター鍵であり、指定鍵ブロックにのみ対応可能となっており、指定鍵ブロック以外の鍵ブロックとの相互認証は成立しない構成となっている。

【0173】

図19から理解されるように、記録デバイス400の内部メモリ405には1～NのN個の鍵ブロックが設定され、各鍵ブロック毎に記録デバイス識別情報、

認証鍵、初期値、保存鍵、乱数生成鍵、種が格納され、少なくとも認証用のかぎデータがブロック毎に異なるデータとして格納されている。

【0174】

このように、記録デバイス400の鍵ブロックの鍵データ構成は、ブロック毎に異なっている。従って、例えば、ある記録再生機器Aが内部メモリに格納された記録デバイス認証鍵用マスター鍵MKakeを用いて認証処理を行ない得る鍵ブロックは鍵ブロックNo. 1であり、また別の仕様の記録再生器Bが認証可能な鍵ブロックは別の鍵ブロック、例えば鍵ブロックNo. 2のように設定することが可能となる。

【0175】

後段でさらに詳細に説明するが、コンテンツを記録デバイス400の外部メモリ402に格納する際、各鍵ブロックに格納された保存鍵Kstrを用いて暗号化処理がなされ、格納されることになる。より、具体的には、コンテンツブロックを暗号化するコンテンツ鍵を保存鍵で暗号化処理する。

【0176】

図19に示すように保存鍵は、各ブロック毎に異なる鍵として構成されている。従って、異なる鍵ブロックを指定するように設定された2つの異なる設定の記録再生器間においては、ある1つの記録デバイスのメモリに格納されたコンテンツを両方で共通に利用することは防止される。すなわち、異なる設定のなされた記録再生器は、それぞれの設定に合致する記録デバイスに格納されたコンテンツのみが利用できる。

【0177】

なお、各鍵ブロックについて共通化可能なデータは共通化することも可能であり、例えば認証用の鍵データ、保存鍵データのみを異なるように構成してもよい。

【0178】

このような記録デバイスに複数の異なる鍵データからなる鍵ブロックを構成する具体例としては、例えば記録再生器300の機種別（据え置き型、携帯型等）で指定すべき鍵ブロック番号を異なるように設定したり、あるいは、アプリケー

ション毎に指定鍵ブロックを異なるように設定する例がある。さらに、例えば日本で販売する記録再生器については指定鍵ブロックをNo. 1とし、米国で販売する記録再生器は指定鍵ブロックをNo. 2とするように地域ごとに異なる鍵ブロック設定を行なう構成とすることも可能である。このような構成とすることで、それぞれの異なる販売地域で使用され、記録デバイスに異なる保存鍵で格納されたコンテンツは、たとえメモ리카ードのような記録デバイスが米国から日本、あるいは日本から米国へ転送されてきても、異なる鍵設定のなされた記録再生器で利用することは不可能であるので、メモリに格納したコンテンツの不正、無秩序な流通を防止できる。具体的には、異なる保存鍵K s t rで暗号化されているコンテンツ鍵K c o nが2国間で相互に利用可能となる状態を排除することができる。

【0179】

さらに、図19に示す記録デバイス400の内部メモリ405の鍵ブロック1～Nまでの少なくとも1つの鍵ブロック、例えばNo. Nの鍵ブロックをいずれの記録再生器300においても共通に利用可能な鍵ブロックとして構成してもよい。

【0180】

例えば、全ての機器に鍵ブロックNo. Nとの認証可能な記録デバイス認証鍵用マスター鍵MK a k eを格納することで、記録再生器300の機種別、アプリケーション毎、仕向け国毎等に関係なく流通可能なコンテンツとして扱うことができる。例えば、鍵ブロックNo. Nに格納された保存鍵でメモ리카ードに格納された暗号化コンテンツは、すべての機器において利用可能なコンテンツとなる。例えば、音楽データ等を共通に利用可能な鍵ブロックの保存鍵で暗号化してメモ리카ードに記憶し、このメモ리카ードを、やはり共通の記録デバイス認証鍵用マスター鍵MK a k eを格納した例えば携帯型の音声再生機器等にセットすることで、メモ리카ードからのデータの復号再生処理を可能とすることができる。

【0181】

本発明のデータ処理装置における複数の鍵ブロックを有する記録デバイスの利用例を図21に示す。記録再生器2101は日本向け製品の記録再生器であり、

記録デバイスの鍵ブロックのNo. 1, 4 との間での認証処理が成立するマスター鍵を持っている。記録再生器 2 1 0 2 は US 向け製品の記録再生器であり、記録デバイスの鍵ブロックのNo. 2, 4 との間での認証処理が成立するマスター鍵を持っている。記録再生器 2 1 0 3 は EU 向け製品の記録再生器であり、記録デバイスの鍵ブロックのNo. 3, 4 との間での認証処理が成立するマスター鍵を持っている。

【0182】

例えば記録再生器 2 1 0 1 は、記録デバイス A, 2 1 0 4 の鍵ブロック 1 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器 2 1 0 2 は、記録デバイス B, 2 1 0 5 の鍵ブロック 2 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。記録再生器 2 1 0 3 は、記録デバイス C, 2 1 0 6 の鍵ブロック 3 または鍵ブロック 4 との間で認証が成立し、それぞれの鍵ブロックに格納された保存鍵を介した暗号処理を施したコンテンツが外部メモリに格納される。ここで、記録デバイス A, 2 1 0 4 を記録再生器 2 1 0 2、または記録再生器 2 1 0 3 に装着した場合、鍵ブロック 1 の保存鍵で暗号処理がなされたコンテンツは、記録再生器 2 1 0 2、記録再生器 2 1 0 3 と鍵ブロック 1 との間での認証が成立しないので利用不可能となる。一方、鍵ブロック 4 の保存鍵で暗号処理がなされたコンテンツは、記録再生器 2 1 0 2、記録再生器 2 1 0 3 と鍵ブロック 4 との間での認証が成立するので利用可能となる。

【0183】

上述のように、本発明のデータ処理装置においては、記録デバイスに複数の異なる鍵セットからなる鍵ブロックを構成し、一方、記録再生機器には、特定の鍵ブロックに対する認証可能なマスター鍵を格納する構成としたので、様々な利用態様に応じたコンテンツの利用制限を設定することが可能となる。

【0184】

なお、1つの記録再生機器において指定可能な鍵ブロックを複数、例えば 1 ~ k とし、他の記録再生器において指定可能な鍵ブロックを p ~ q のように複数と

することも可能であり、また、共通に利用可能な鍵ブロックを複数設ける構成としてもよい。

【0185】

(7) 記録再生器から記録デバイスへのダウンロード処理

次に、本発明のデータ処理装置において、記録再生器300から記録デバイス400の外部メモリにコンテンツをダウンロードする処理について説明する。

【0186】

図22は、記録再生器300から記録デバイス400へコンテンツをダウンロードする手順を説明する流れ図である。なお、図22においては、既に記録再生器300と記録デバイス400との間で上述した相互認証処理が完了しているものとする。

【0187】

ステップS51において、記録再生器300の制御部301は、読み取り部304を使ってコンテンツを格納したメディア500から所定のフォーマットに従ったデータを読み出さか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信する。そして、記録再生器300の制御部301は、データの内のヘッダ (Header) 部分 (図4参照) を記録再生器300の記録再生器暗号処理部302に送信する。

【0188】

次に、ステップS52において、ステップS51でヘッダ (Header) を受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図7で説明したICV計算方法に従って計算される。なお、初期値は、 $IV = 0$ としても、記録再生器暗号処理部302の内部メモリ307にチェック値A生成用初期値IVaを保存しておき、それを使用してもよい。最後に、チェック値Aとヘッダ (Header) 内に格納されたチェック値: ICVaを比較し、一致していた場合にはステップS53へ進む。

【0189】

先に図4において説明したようにチェック値A、ICVaは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵Kicvaを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICVaと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

【0190】

次に、ステップS53において、記録再生器暗号処理部302の制御部306は、配送鍵Kdisの生成を記録再生器暗号処理部302の暗号/復号化部308に行わせる。配送鍵Kdisの生成方法としては、例えば次のように生成する。

【0191】

【数4】

$$Kdis = DES(MKdis, ContentID \wedge IVdis)$$

【0192】

ここで、MKdisは、配送鍵Kdisを生成するための配送鍵用マスター鍵であり、これは、前述したように記録再生器300の内部メモリに格納されている鍵である。またContent IDはコンテンツデータのヘッダ部の識別情報であり、さらにIVdisは、配送鍵用初期値である。また、上記式において、DES()は、第1引数を暗号鍵として、第2引数の値を暗号化する関数であり、演算 \wedge は64ビット単位の排他的論理和を示す。

【0193】

ステップS54において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308を使って、ステップS53で生成した配送鍵Kdisを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘ

ッダ部に格納されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} (図4 参照) の復号化処理を行う。図4 に示されるようにこれらブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、配送鍵 K_{dis} によって予め暗号化処理が施されている。

【0194】

さらに、ステップ S55 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 を使って、ステップ S54 で復号化したブロック情報鍵 K_{bit} でブロック情報 (BIT) を復号化する。図4 に示されるようにブロック情報 (BIT) は、DVD、CD等のメディア、あるいはインターネット等の通信路上では、ブロック情報鍵 K_{bit} によって予め暗号化処理が施されている。

【0195】

さらに、ステップ S56 において、記録再生器暗号処理部 302 の制御部 306 は、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} およびブロック情報 (BIT) を 8 バイト単位に分割し、それら全てを排他的論理和する (加算、減算等、いずれの演算でもよい)。次に、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にチェック値 B (ICVb) を計算させる。チェック値 B は、図24 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 B 生成鍵 K_{icvb} を鍵とし、先ほど計算した排他的論理和値を DES で暗号化して生成する。最後に、チェック値 B と Header 内の ICVb を比較し、一致していた場合にはステップ S57 へ進む。

【0196】

先に図4 において説明したように、チェック値 B 、ICVb は、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報 (BIT) の改竄を検証するためのチェック値である。記録再生器暗号処理部 302 の内部メモリ 307 に保存されているチェック値 B 生成鍵 K_{icvb} を鍵とし、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} およびブロック情報 (BIT) を 8 バイト単位に分割し排他的論理和して得られる値を DES で暗号化して生成したチェック値 B が、ヘ

ッダ (Header) 内に格納されたチェック値: ICV_b と一致した場合には、ブロック情報鍵 K_{bit} 、コンテンツ鍵 K_{con} 、ブロック情報の改竄はないと判断される。

【0197】

ステップ S57 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に中間チェック値の計算をさせる。中間チェック値は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されている総チェック値生成鍵 K_{icvt} を鍵とし、検証したヘッダ (Header) 内のチェック値 A、チェック値 B、保持しておいた全てのコンテンツチェック値をメッセージとして図 7 で説明した ICV 計算方法に従って計算する。なお、初期値 $IV=0$ としても、記録再生器暗号処理部 302 の内部メモリ 307 に総チェック値生成用初期値 IV_t を保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器 300 の記録再生器暗号処理部 302 に保持しておく。

【0198】

この中間チェック値は、チェック値 A、チェック値 B、全てのコンテンツチェック値をメッセージとして生成されるものであり、これらの各チェック値の検証対象となっているデータについての検証を中間チェック値の照合処理によって行なってもよい。しかし、本実施例においては、システム全体の共有データとしての非改竄性検証処理と、ダウンロード処理後に各記録再生機器 300 のみが占有する占有データとして識別するための検証処理を区別して実行可能とするために、中間チェック値からさらに複数の異なるチェック値、すなわち総チェック値 ICV_t と、記録再生器固有チェック値 ICV_{dev} とを別々に、中間チェック値に基づいて生成可能としている。これらのチェック値については後段で説明する。

【0199】

記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値 ICV_t の計算をさせる。総チェック値 ICV_t は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 3

07に保存されているシステム署名鍵K s y sを鍵とし、中間チェック値をDESで暗号化して生成する。最後に、生成した総チェック値ICVtとステップS51で保存しておいたHeader内のICVtを比較し、一致していた場合には、ステップS58へ進む。システム署名鍵K s y sは、複数の記録再生器、すなわちある一定のデータの記録再生処理を実行するシステム集合全体において共通する署名鍵である。

【0200】

先に図4において説明したように、総チェック値ICVtは、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値：ICVtと一致した場合には、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【0201】

次に、ステップS58において、記録再生器300の制御部301は、ブロック情報(BIT)内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

【0202】

コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録再生器300の読み取り部304を使ってメディア500から読み出すか、記録再生器300の通信部305を使って通信手段600から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツ中間値を計算させる。

【0203】

コンテンツ中間値は、ステップS54で復号化したコンテンツ鍵Kconで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトごとに区切り、全て排他的論理和(加算、減算等、いずれの演算でもよ

い) して生成する。

【0204】

次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部302の内部メモリ307に保存されているコンテンツチェック値生成鍵 K_{icvc} を鍵とし、コンテンツ中間値をDESで暗号化して生成する。そして、記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS51で記録再生器300の制御部301から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、Header生成側と合わせておけば、 $IV=0$ としても、記録再生器暗号処理部302の内部メモリ307にコンテンツチェック値生成用初期値 IV_c を保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器300の記録再生器暗号処理部302に保持しておく。さらにまた、記録再生器300の記録再生器暗号処理部302は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。そして、全ての検証が成功した場合には、ステップS59へ進む。

【0205】

次に、ステップS59において、記録再生器300の記録再生器暗号処理部302は、ステップS54で復号化しておいたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を、記録再生器暗号処理部302の暗号／復号化部308に、相互認証の際に共有しておいたセッション鍵 K_{ses} で暗号化させる。記録再生器300の制御部301は、セッション鍵 K_{ses} で暗号化されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントロー

ラ 303 を介して記録デバイス 400 に送信する。

【0206】

次に、ステップ S60 において、記録再生器 300 から送信されてきたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を受信した記録デバイス 400 は、受信したデータを記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵 K s e s で復号化させ、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K s t r で再暗号化させる。最後に、記録再生器 300 の制御部 301 は、記録再生器 300 の記録デバイスコントローラ 303 を介し、記録デバイス 400 から保存鍵 K s t r で再暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n を読み出す。そして、これらの鍵を、配送鍵 K d i s で暗号化されたブロック情報鍵 K b i t とコンテンツ鍵 K c o n に置き換える。

【0207】

ステップ S61 において、記録再生器 300 の制御部 301 は、データのヘッダ部の取扱方針 (Usage Policy) から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器 300 のみで利用できる（この場合、利用制限情報が 1 に設定）か、別の同様な記録再生器 300 でも利用できる（この場合、利用制限情報が 0 に設定）か判定する。判定の結果、利用制限情報が 1 であった場合には、ステップ S62 に進む。

【0208】

ステップ S62 において、記録再生器 300 の制御部 301 は、記録再生器固有のチェック値を記録再生器 300 の記録再生器暗号処理部 302 に計算させる。記録再生器固有のチェック値は、図 25 に示すように記録再生器暗号処理部 302 の内部メモリ 307 に保存されている記録再生器署名鍵 K d e v を鍵とし、ステップ S58 で保持しておいた中間チェック値を D E S で暗号化して生成する。計算された記録再生器固有のチェック値 I C V d e v は、総チェック値 I C V t の代わりに上書きされる。

【0209】

先に説明したように、システム署名鍵 K s y s は、配信システムに共通の署名

またはICVをつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵Kdevは、記録再生器毎に異なり、記録再生器が署名またはICVをつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵Ksysによって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値ICVtが一致することになるので、共通に利用可能となるが、記録再生器署名鍵Kdevを用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵Kdevを用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値ICVdevが不一致となり、エラーとなるので再生できないことになる。

【0210】

従って、本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

【0211】

ステップS63において、記録再生器300の制御部301は、コンテンツを記録デバイス400の外部メモリ402に保存する。

【0212】

図26は、利用制限情報が0の場合における記録デバイス内のコンテンツ状況を示す図である。図27は、利用制限情報が1の場合における記録デバイス内のコンテンツ状況を示す図である。図26が図4と異なる点は、コンテンツブロック情報鍵Kbitとコンテンツ鍵Kconが配送鍵Kdisで暗号化されているか、保存鍵Kstrで暗号化されているかだけである。また、図27が図26と異なる点は、中間チェック値から計算されるチェック値が、図26ではシステム署名鍵Ksysで暗号化されているのに対し、図27では記録再生器固有の記録再生器署名鍵Kdevで暗号化されていることである。

【0213】

なお、図22の処理フローにおいて、ステップS52でチェック値Aの検証に

失敗した場合、ステップ S 5 6 でチェック値 B の検証に失敗した場合、ステップ S 5 7 で総チェック値 I C V t の検証に失敗した場合、ステップ S 5 8 で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合には、ステップ S 6 4 に進み、所定のエラー表示を行う。

【 0 2 1 4 】

また、ステップ S 6 1 で利用制限情報が 0 であった場合には、ステップ S 6 2 をスキップしてステップ S 6 3 へ進む。

【 0 2 1 5 】

(8) 記録デバイス格納情報の記録再生器での再生処理

次に記録デバイス 4 0 0 の外部メモリ 4 0 2 に格納されたコンテンツ情報の記録再生器 3 0 0 での再生処理について説明する。

【 0 2 1 6 】

図 2 8 は、記録再生器 3 0 0 が記録デバイス 4 0 0 からコンテンツを読み出し、コンテンツを利用する手順を説明する流れ図である。なお、図 2 8 においても、既に記録再生器 3 0 0 と記録デバイス 4 0 0 との間で相互認証が完了しているものとする。

【 0 2 1 7 】

ステップ S 7 1 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイスコントローラ 3 0 3 を使って記録デバイス 4 0 0 の外部メモリ 4 0 2 からコンテンツを読み出す。そして、記録再生器 3 0 0 の制御部 3 0 1 は、データの内のヘッダ (Header) 部分を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に送信する。ステップ S 7 2 は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップ S 5 2 と同様の処理であり、ヘッダ (Header) を受信した記録再生器暗号処理部 3 0 2 の制御部 3 0 6 が、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 にチェック値 A を計算させる処理である。チェック値 A は、先に説明した図 2 3 に示すように記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されているチェック値 A 生成鍵 K i c v a を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして図 7 で説明したと同様の I C V 計算方法に従って計算される。

【0218】

先に説明したようにチェック値A、ICV aは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7で説明したICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICV aと一致した場合には、記録デバイス400に格納された識別情報、取扱方針の改竄はないと判断される。

【0219】

次に、ステップS73において、記録再生器300の制御部301は、読み出したヘッダ(Header)部分からブロック情報鍵K b i tとコンテンツ鍵K c o nを取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。記録再生器300から送信されてきたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号/復号化部406に、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K s t rで復号化処理させ、相互認証の際に共有しておいたセッション鍵K s e sで再暗号化させる。そして、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400からセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを読み出す。

【0220】

次に、ステップS74において、記録再生器300の制御部301は、受信したセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを記録再生器300の記録再生器暗号処理部302に送信する。

【0221】

セッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の暗号/復号化部308に、セッション鍵K s e sで暗

号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを、相互認証の際に共有しておいたセッション鍵K s e sで復号化させる。そして、復号化したブロック情報鍵K b i tで、ステップS 7 1で受信しておいたブロック情報を復号化させる。

【0222】

なお、記録再生器300の記録再生器暗号処理部302は、復号化したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tを、ステップS 7 1で受信しておいたブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器300の制御部301は、復号化されたブロック情報B I Tを記録再生器300の記録再生器暗号処理部302から読み出しておく。

【0223】

ステップS 7 5は、「(7) 記録再生器から記録デバイスへのダウンロード処理」において説明したステップS 5 6と同様の処理である。記録再生器暗号処理部302の制御部306が、記録デバイス400から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単位に分割し、それら全てを排他的論理和する。次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308にチェック値B(I C V b)を計算させる。チェック値Bは、先に説明した図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、先ほど計算した排他的論理和値をDESで暗号化して生成する。最後に、チェック値BとHeader内のI C V bを比較し、一致していた場合にはステップS 7 6へ進む。

【0224】

先に説明したように、チェック値B, I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、記録デバイス400から読み出したブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報(B I T)を8バイト単

位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、記録デバイス400から読み出したデータ中のヘッダ(Header)内に格納されたチェック値:ICVbと一致した場合には、記録デバイス400に格納されたデータのブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄はないと判断される。

【0225】

ステップS76において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号/復号化部308に中間チェック値の計算をさせる。中間チェック値は、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したヘッダ(Header)内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7他で説明したICV計算方法に従って計算する。なお、初期値はIV=0としても、記録再生器暗号処理部302の内部メモリ307に総チェック値生成用初期値にIVtを保存しておき、それを使用してもよい。また、生成した中間チェック値は、必要に応じて記録再生器300の記録再生器暗号処理部302に保持しておく。

【0226】

次に、ステップS77において、記録再生器300の制御部301は、記録デバイス400の外部メモリ402から読み出したデータのヘッダ部に含まれる取扱方針(Usage Policy)から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる(利用制限情報が1)か、別の同様な記録再生器300でも利用できる(利用制限情報が0)か判定する。判定の結果、利用制限情報が1、すなわちダウンロードしたコンテンツが当該記録再生器300のみで利用できる利用制限が設定されている場合には、ステップS80に進み、利用制限情報が0、すなわち別の同様な記録再生器300でも利用できる設定であった場合には、ステップS78に進む。なお、ステップS77の処理は、暗号処理部302が行なってもよい。

【0227】

ステップS78においては、(7)記録再生器から記録デバイスへのダウンロ

ード処理において説明したステップS58と同様の総チェック値ICVtの計算が実行される。すなわち、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に総チェック値ICVtの計算をさせる。総チェック値ICVtは、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵Ksysを鍵とし、中間チェック値をDESで暗号化して生成する。

【0228】

次に、ステップS79に進み、ステップS78において生成した総チェック値ICVtとステップS71で保存しておいたヘッダ(Header)内のICVtを比較し、一致していた場合には、ステップS82へ進む。

【0229】

先に説明したように、総チェック値ICVtは、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値：ICVtと一致した場合には、記録デバイス400に格納されたデータにおいて、ICVa、ICVb、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【0230】

ステップS77での判定において、ダウンロードしたコンテンツが当該記録再生器300のみで利用できる設定であった場合、すなわち設定情報が1であった場合は、ステップS80に進む。

【0231】

ステップS80において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に、記録再生器固有のチェック値ICVdevの計算をさせる。記録再生器固有のチェック値ICVdevは、先に説明した図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器固有の記録再生器署名鍵Kdevを鍵とし、中間チェック値をDESで暗号化して生成する。ステップS81において、ステップS80で計算した記録再生器固有のチェック値ICVdevとステップS71

で保存しておいたHeader内の I C V d e v を比較し、一致していた場合には、ステップ S 8 2 へ進む。

【 0 2 3 2 】

このように、システム署名鍵 K s y s によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値 I C V t が一致することになるので共通に利用可能となり、記録再生器署名鍵 K d e v を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵 K d e v を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装着して再生しようとした場合、記録再生器固有のチェック値 I C V d e v が不一致となり、エラーとなるので再生できないことになる。従って、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定することが可能となる。

【 0 2 3 3 】

ステップ S 8 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、ステップ S 7 4 で読み出しておいたブロック情報 B I T 内のコンテンツブロック情報を取り出し、コンテンツブロックが暗号化対象になっているかいないか調べる。暗号化対象になっていた場合には、該当するコンテンツブロックを、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介し、記録デバイス 4 0 0 の外部メモリ 4 0 2 から読み出し、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 へ送信する。これを受信した記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 にコンテンツを復号化させるとともに、コンテンツブロックが検証対象になっている場合には次のステップ S 8 3 においてコンテンツチェック値を検証させる。

【 0 2 3 4 】

ステップ S 8 3 は、「（ 7 ）記録再生器から記録デバイスへのダウンロード処理」において説明したステップ S 5 8 と同様の処理である。記録再生器 3 0 0 の制御部 3 0 1 は、ブロック情報（ B I T ）内のコンテンツブロック情報を取り出

し、コンテンツブロックが検証対象になっているかいないかをコンテンツチェック値の格納状況から判定し、コンテンツブロックが検証対象になっていた場合には、該当するコンテンツブロックを、記録デバイス400の外部メモリ402から受信し、記録再生器300の記録再生器暗号処理部302へ送信する。これを受信した記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツ中間値を計算させる。

【0235】

コンテンツ中間値は、ステップS74で復号化したコンテンツ鍵Kconで、入力されたコンテンツブロックをDESのCBCモードで復号化し、その結果を8バイトに区切り全て排他的論理和して生成する。

【0236】

次に、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308にコンテンツチェック値の計算をさせる。コンテンツチェック値は、記録再生器暗号処理部302の内部メモリ307に保存されているコンテンツチェック値生成鍵Kicvcを鍵とし、コンテンツ中間値をDESで暗号化して生成する。そして、記録再生器暗号処理部302の制御部306は、当該コンテンツチェック値と、ステップS71で記録再生器300の制御部301から受信したコンテンツブロック内のICVを比較し、その結果を記録再生器300の制御部301に渡す。これを受信した記録再生器300の制御部301は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す。なお、初期値はIV=0としても、記録再生器暗号処理部302の内部メモリ307にコンテンツチェック値生成用初期値IVcを保存しておき、それを使用してもよい。また、チェックした全てのコンテンツチェック値は、記録再生器300の記録再生器暗号処理部302に保持しておく。さらにまた、記録再生器300の記録再生器暗号処理部302は、検証対象のコンテンツブロックの検証順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上検証させられたりした場合には、認証に失敗したものとする。

【0237】

記録再生器300の制御部301は、当該コンテンツチェック値の比較結果（検証対象になっていない場合、比較結果は全て成功とする）を受信し、検証に成功していた場合には、記録再生器300の記録再生器暗号処理部302から復号化されたコンテンツを取り出す。そして、次の復号化対象コンテンツブロックを取り出して記録再生器300の記録再生器暗号処理部302に復号化させ、全てのコンテンツブロックを復号化するまで繰り返す。

【0238】

なお、ステップS83において、記録再生器300の記録再生器暗号処理部302は、コンテンツチェック値の検証処理において不一致となった場合には、検証失敗としてその時点で処理を中止し、残るコンテンツの復号化は行わない。また、記録再生器300の記録再生器暗号処理部302は、復号化対象のコンテンツブロックの復号化順序を監視し、順序が間違っていたり、同一のコンテンツブロックを2回以上復号化させられたりした場合には、復号化に失敗したものとする。

【0239】

なお、ステップS72でチェック値Aの検証に失敗した場合、ステップS75でチェック値Bの検証に失敗した場合、ステップS79で総チェック値ICV_tの検証に失敗した場合、ステップS81で記録再生器固有のチェック値ICV_d_e_vの検証に失敗した場合には、ステップS83で各コンテンツブロックのコンテンツチェック値の検証に失敗した場合、ステップS84に進み、所定のエラー表示を行う。

【0240】

以上説明してきたように、コンテンツをダウンロードしたり、利用したりする際に、重要なデータやコンテンツを暗号化しておいて隠蔽化したり、改竄検証ができるだけでなく、ブロック情報BITを復号化するためのブロック情報鍵K_b_i_t、コンテンツを復号化するためのコンテンツ鍵K_c_o_nが記録デバイス固有の保存鍵K_s_t_rで保存されているため、単純に記録メディア上のデータを別の記録メディアに複製したとしても、コンテンツを正しく復号化することができな

くすることができる。より具体的には、例えば図28のステップS74において、記録デバイス毎に異なる保存鍵Kstrで暗号化されたデータを復号化するため、別の記録デバイスではデータを正しく復号化できない構成を持つからである。

【0241】

(9) 相互認証後の鍵交換処理

本発明のデータ処理装置における特徴の1つに、上述した記録再生器300と記録デバイス400との間で実行される相互認証処理の後においてのみ、記録デバイスの利用を可能とし、また、その利用態様を制限した点がある。

【0242】

例えば、不正な複製等によってコンテンツを格納したメモリカード等の記録デバイスを生成し、これを記録再生器にセットして利用されることを排除するために、記録再生器300と、記録デバイス400間での相互認証処理を実行し、かつ認証OKとなったことを条件として、コンテンツ（暗号化された）の記録再生器300および記録デバイス400間での転送を可能としている。

【0243】

上記の制限的処理を実現するために、本発明のデータ処理装置においては、記録デバイス400の暗号処理部401での処理は、すべて、予め設定されたコマンド列に基づいて実行される構成となっている。すなわち、記録デバイスは、コマンド番号に基づくコマンドを順次レジスタから取り出して実行するコマンド処理構成を持つ。この記録デバイスでのコマンド処理構成を説明する図を図29に示す。

【0244】

図29に示すように記録再生器暗号処理部302を有する記録再生器300と記録デバイス暗号処理部401を有する記録デバイス400間においては、記録再生器300の制御部301の制御のもとに記録デバイスコントローラ303から記録デバイス400の通信部(受信レジスタを含む)404に対してコマンド番号(N o .)が出力される。

【0245】

記録デバイス400は、暗号処理部401内の制御部403にコマンド番号管理部2201を有する。コマンド番号管理部2901は、コマンドレジスタ2902を保持しており、記録再生器300から出力されるコマンド番号に対応するコマンド列を格納している。コマンド列は、図29の右に示すようにコマンド番号0からyまで順次、コマンド番号に対して実行コマンドが対応付けされている。コマンド番号管理部2901は、記録再生器300から出力されるコマンド番号を監視し、対応するコマンドをコマンドレジスタ2902から取り出して実行する。

【0246】

コマンドレジスタ2902に格納されたコマンドシーケンスは、図29の右に示すように、認証処理シーケンスに関するコマンド列が先行するコマンド番号0～kに対応付けられている。さらに、認証処理シーケンスに関するコマンド列の後のコマンド番号p～sに復号、鍵交換、暗号処理コマンドシーケンス1、さらに、後続するコマンド番号u～yに復号、鍵交換、暗号処理コマンドシーケンス2が対応付けされている。

【0247】

先に図20の認証処理フローにおいて説明したように、記録デバイス400が記録再生器300に装着されると、記録再生器300の制御部301は、記録デバイスコントローラ303を介して記録デバイス400に初期化命令を送信する。これを受信した記録デバイス400は、記録デバイス暗号処理部401の制御部403において、通信部404を介して命令を受信し、認証フラグ2903をクリアする。すなわち未認証状態に設定する。または、記録再生器300から記録デバイス400に電源が供給される様な場合には、パワーオン時に未承認状態としてセットを行なう方式でもよい。

【0248】

次に、記録再生器300の制御部301は、記録再生器暗号処理部302に初期化命令を送信する。このとき、記録デバイス挿入口番号も併せて送信する。記録デバイス挿入口番号を送信することにより、記録再生器300に複数の記録デバイスが接続された場合であっても同時に複数の記録デバイス400との認証処

理、およびデータ送受信が可能となる。

【0249】

初期化命令を受信した記録再生器300の記録再生器暗号処理部302は、記録再生器暗号処理部302の制御部において、記録デバイス挿入口番号に対応する認証フラグ2904をクリアする。すなわち未認証状態に設定する。

【0250】

これらの初期化処理が完了すると、記録再生器300の制御部301は、記録デバイスコントローラ303を介してコマンド番号0から順次コマンド番号を昇順に出力する。記録デバイス400のコマンド番号管理部2901は、記録再生器300から入力されるコマンド番号を監視し、0から順次入力されることを確認して、対応するコマンドをコマンドレジスタ2902から取り出して認証処理等各種処理を実行する。入力されるコマンド番号が規定の順でなかった場合には、エラーとし、コマンド番号受付値を初期状態、すなわち実行可能コマンド番号=0にリセットする。

【0251】

図29に示すようにコマンドレジスタ2902に格納されたコマンドシーケンスは、認証処理を先行して処理するようにコマンド番号が付与されており、その後の処理に復号、鍵交換、暗号化処理の処理シーケンスが格納されている。

【0252】

復号、鍵交換、暗号化処理の処理シーケンスの具体例を図30、31を用いて説明する。

【0253】

図30は、先に図22において説明した記録再生器300から記録デバイス400へのコンテンツのダウンロード処理において実行される処理の一部を構成するものである。具体的には図22におけるステップS59～S60の間で実行される

【0254】

図30において、ステップS3001は、記録再生器からセッション鍵K_{se}で暗号化されたデータ（ex. ブロック情報鍵K_{bit}、コンテンツ鍵K_{co}

n) を記録デバイスが受信する処理であり、その後、前述の図29で示したコマンド列p～sが開始される。コマンド列p～sは認証処理コマンド0～kが完了し、図29に示す認証フラグ2903、2904に認証済みのフラグがセットされた後開始される。これは、コマンド番号管理部2901がコマンド番号を0から昇順でのみ受け付けることによって保証される。

【0255】

ステップS3002は、記録デバイスが記録再生器から受信したセッション鍵Ksesで暗号化されたデータ(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)をレジスタに格納する処理である。

【0256】

ステップS3003は、セッション鍵Ksesで暗号化されたデータ(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)をレジスタから取り出してセッション鍵Ksesで復号する処理を実行するステップである。

【0257】

ステップS3004は、セッション鍵Ksesで復号化されたデータ(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)を保存鍵Kstrで暗号化する処理を実行するステップである。

【0258】

上記の処理ステップ3002～3004は、先の図29で説明したコマンドレジスタ中のコマンド番号p～sに含まれる処理である。これらの処理は、記録デバイス400のコマンド番号管理部2901において記録再生器300から受信するコマンド番号p～sに従って記録デバイス暗号処理部401が順次実行する。

【0259】

次のステップS3005は、保存鍵Kstrで暗号化したデータ(ex. ブロック情報鍵Kbit, コンテンツ鍵Kcon)を記録デバイスの外部メモリに格納するステップである。このステップにおいては、記録デバイス暗号処理部401から記録再生器300が保存鍵Kstrで暗号化したデータを読み出して、その後、記録デバイス400の外部メモリ402に格納してもよい。

【0260】

上述のステップS3002～S3004は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3003の復号処理終了時点で、記録再生器300からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号p～sに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データ、コンテンツの不正な読み出しを防止できる。

【0261】

図31は、先に図28において説明した記録デバイス400からコンテンツを読み出して記録再生器300において再生するコンテンツ再生処理において実行される処理の一部を構成するものである。具体的には図28におけるステップS73において実行される処理である。

【0262】

図31において、ステップS3101は、記録デバイス400の外部メモリ402から保存鍵Kstrで暗号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）の読み出しを実行するステップである。

【0263】

ステップS3102は、記録デバイスのメモリから読み出した保存鍵Kstrで暗号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をレジスタに格納するステップである。このステップにおいては、記録デバイス400の外部メモリ402から記録再生器300が保存鍵Kstrで暗号化したデータを読み出して、その後に記録デバイス400のレジスタに格納してもよい。

【0264】

ステップS3103は、保存鍵Kstrで暗号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をレジスタから取り出して保存鍵Kstrで復号処理するステップである。

【0265】

ステップS3104は、保存鍵Kstrで復号化されたデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）をセッション鍵Ksesで暗号化処理するステップである。

【0266】

上記の処理ステップ3102～3104は、先の図29で説明したコマンドレジスタ中のコマンド番号u～yに含まれる処理である。これらの処理は、記録デバイスのコマンド番号管理部2901において記録再生器300から受信するコマンド番号u～yに従って記録デバイス暗号処理部406が順次実行する。

【0267】

次のステップS3105は、セッション鍵Ksesで暗号化したデータ（ex. ブロック情報鍵Kbit、コンテンツ鍵Kcon）を記録デバイスから記録再生器へ送信する処理である。

【0268】

上述のステップS3102～S3104は、連続して実行される割込み不可能な実行シーケンスであり、たとえば、ステップS3103の復号処理終了時点で、記録再生器300からのデータ読み出し命令があったとしても、その読み出しコマンドは、コマンドレジスタ2902のコマンド番号u～yに設定された昇順のコマンド番号とは異なるため、コマンド番号管理部2901は、読み出しの実行を受け付けない。従って、記録デバイス400における鍵交換の際に発生する復号データを外部、例えば記録再生器300から読み出すことは不可能となり、鍵データあるいはコンテンツの不正な読み出しを防止できる。

【0269】

なお、図30、31に示す処理では、鍵交換によって復号、暗号化される対象が、ブロック情報鍵Kbit、コンテンツ鍵Kconである例を示したが、これらの図29に示したコマンドレジスタ2902に格納されたコマンドシーケンスには、コンテンツ自体の鍵交換を伴う復号、暗号化処理を含ませてもよく、鍵交換によって復号、暗号化される対象は上述の例に限定されるものではない。

【0270】

以上、本発明のデータ処理装置における相互認証後の鍵交換処理について説明した。このように、本発明のデータ処理装置における鍵交換処理は、記録再生器と記録デバイス間での認証処理が終了した後においてのみ実行可能となり、さらに、鍵交換処理における復号データの外部からのアクセスが防止可能な構成となっているので、コンテンツ、鍵データの高度なセキュリティが確保される。

【0271】

(10) 複数のコンテンツデータフォーマットと、各フォーマットに対応するダウンロードおよび再生処理

上述した実施例では、例えば図3に示すメディア500あるいは通信手段600におけるデータフォーマットが図4に示す1つの種類である場合について説明してきた。しかしながら、メディア500あるいは、通信手段600におけるデータフォーマットは、上述の図4に示すフォーマットに限らず、コンテンツが音楽である場合、画像データである場合、ゲーム等のプログラムである場合等、コンテンツに応じたデータフォーマットを採用することが望ましい。以下、複数の異なるデータフォーマットと、各フォーマットに対応する記録デバイスへのダウンロード処理および記録デバイスからの再生処理について説明する。

【0272】

図32～35に4つの異なるデータフォーマットを示す。各図の左側には、図3に示すメディア500、または通信手段600上におけるデータフォーマットを、また各図の右側には記録デバイス400の外部メモリ402に格納される場合のデータフォーマットを示してある。先に、図32～35に示すデータフォーマットの概略を説明し、その後、各フォーマットにおける各データの内容、および各フォーマットにおけるデータの差異について説明する。

【0273】

図32は、フォーマットタイプ0であり、上述の説明中で例として示したタイプと共通のものである。このフォーマットタイプ0の特徴は、データ全体を任意の大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割し、各ブロックについて任意に暗号化し、暗号化ブロックと非暗号化ブロック、すなわち平文ブロックを混在させてデータを構成できる点である。ブロックの暗号化

は、コンテンツ鍵 K_{con} によって実行されており、コンテンツ鍵 K_{con} は、メディア上では配送鍵 K_{dis} によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 K_{str} によって暗号化される。ブロック情報鍵 K_{bit} についてもメディア上では配送鍵 K_{dis} によって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵 K_{str} によって暗号化される。これらの鍵交換は、前述の「(9) 相互認証後の鍵交換処理」において説明した処理にしたがって実行される。

【0274】

図33は、フォーマットタイプ1であり、このフォーマットタイプ1は、フォーマットタイプ0と同様、データ全体をN個のデータブロック、すなわちブロック1～ブロックNに分割しているが、N個の各ブロックの大きさを同じ大きさとした点で前述のフォーマットタイプ0と異なる。コンテンツ鍵 K_{con} によるブロックの暗号化処理態様は前述のフォーマットタイプ0と同様である。また、メディア上で配送鍵 K_{dis} によって暗号化され、記録デバイスにおける保存時には記録デバイスの内部メモリに格納された保存鍵 K_{str} によって暗号化されるコンテンツ鍵 K_{con} およびブロック情報鍵 K_{bit} 構成も上述のフォーマットタイプ0と同様である。フォーマットタイプ1は、フォーマットタイプ0と異なり、固定的なブロック構成としたことで、ブロック毎のデータ長等の構成データが簡略化されるので、フォーマットタイプ0に比較してブロック情報のメモリサイズを減らすことが可能となる。

【0275】

図33の構成例では、各ブロックを暗号化パートと非暗号化（平文）パートの1組によって構成している。このようにブロックの長さ、構成が規則的であれば、復号処理等の際に各ブロック長、ブロック構成を確認する必要がなくなるので効率的な復号、暗号処理が可能となる。なお、フォーマット1においては、各ブロックを構成するパート、すなわち暗号化パート、非暗号化（平文）パートは、各パート毎にチェック対象として定義可能な構成となっており、要チェックパーツを含むブロックである場合は、そのブロックに関してコンテンツチェック値I

CViが定義される。

【0276】

図34は、フォーマットタイプ2であり、このフォーマットタイプ2の特徴は、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵Kb1cで暗号化されていることである。各ブロック鍵Kb1cの暗号化は、コンテンツ鍵Kconによって実行されており、コンテンツ鍵Kconは、メディア上では配送鍵Kdisによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Kstrによって暗号化される。ブロック情報鍵Kbitについてもメディア上では配送鍵Kdisによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Kstrによって暗号化される。

【0277】

図35は、フォーマットタイプ3であり、このフォーマットタイプ3の特徴は、フォーマット・タイプ2と同様、同じ大きさのN個のデータブロック、すなわちブロック1～ブロックNに分割され、各ブロックについて、それぞれ個別のブロック鍵Kb1cで暗号化されていること、さらに、コンテンツ鍵を用いず、各ブロック鍵Kb1cの暗号化は、メディア上では配送鍵Kdisによって暗号化され、記録デバイス上では保存鍵Kstrによって暗号化されている点である。コンテンツ鍵Kconは、メディア上、デバイス上、いずれにも存在しない。ブロック情報鍵Kbitはメディア上では配送鍵Kdisによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵Kstrによって暗号化される。

【0278】

次に、上記フォーマットタイプ0～3のデータの内容について説明する。データは先に説明したように、ヘッダ部とコンテンツ部に大きく2つに分類され、ヘッダ部にはコンテンツ識別子、取扱方針、チェック値A、B、総チェック値、ブロック情報鍵、コンテンツ鍵、ブロック情報が含まれる。

【0279】

取扱方針には、コンテンツのデータ長、ヘッダ長、フォーマットタイプ（以下説明するフォーマット0～3）、例えばプログラムであるか、データであるか等のコンテンツタイプ、前述のコンテンツの記録デバイスへのダウンロード、再生の欄で説明したように、コンテンツが記録再生器固有に利用可能か否かを決定するフラグであるローカリゼーション・フラグ、さらに、コンテンツのコピー、ムーブ処理に関する許可フラグ、さらに、コンテンツ暗号化アルゴリズム、モード等、コンテンツに関する各種の利用制限情報および処理情報を格納する。

【0280】

チェック値A：ICV aは、識別情報、取扱方針に対するチェック値であり、例えば、前述の図23で説明した手法によって生成される。

【0281】

ブロック情報鍵K b i tは、ブロック情報を暗号化するための鍵であり、先に説明したように、メディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。

【0282】

コンテンツ鍵K c o nは、コンテンツの暗号化に用いる鍵であり、フォーマットタイプ0, 1では、ブロック情報鍵K b i tと同様にメディア上では配送鍵K d i sによって暗号化され、記録デバイスにおける保存時には、記録デバイスの内部メモリに格納された保存鍵K s t rによって暗号化される。なお、フォーマットタイプ2では、コンテンツ鍵K c o nは、コンテンツ各ブロックに構成されるブロック鍵K b l cの暗号化にも利用される。また、フォーマット・タイプ3においては、コンテンツ鍵K c o nは存在しない。

【0283】

ブロック情報は、個々のブロックの情報を記述するテーブルであり、ブロックの大きさ、暗号化されているか否かについてのフラグ、すなわち各ブロックがチェックの対象（ICV）と、なっているか否かを示す情報が格納される。ブロックがチェックの対象となっている場合は、ブロックのチェック値ICV i（ブロックiのチェック値）がテーブル中に定義されて格納される。このブロック情報

は、ブロック情報暗号鍵 K_{bit} によって暗号化される。

【0284】

なお、ブロックのチェック値、すなわちコンテンツチェック値 ICV_i は、ブロックが暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値を記録再生器300の内部メモリ307に格納されたコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、ブロックが暗号化されていない場合は、ブロックデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。図36にコンテンツブロックのチェック値 ICV_i を生成する構成例を示す。メッセージ M の各々が復号文データまたは平文データの各8バイトを構成する。

【0285】

なお、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値 ICV_i の対象データ、すなわち要チェックパーツである場合は、そのブロックに関してコンテンツチェック値 ICV_i が定義される。ブロック i におけるパーツ j のチェック値 $P-ICV_{ij}$ は、パーツ j が暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵 K_{icvc} で暗号化した値として生成される。また、パーツ j が暗号化されていない場合は、パーツのブロックのデータ（平文）の全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。

【0286】

さらに、1つのブロック i 内にチェック対象であることを示す [ICV フラグ = $subject\ of\ ICV$] であるパーツ、すなわち要チェックパーツが1つのみ存在する場合は、上述の手法で生成したチェック値 $P-ICV_{ij}$ をそのままブロックのチェック値 ICV_i とし、また、1つのブロック i 内にチェック対象であることを示す [ICV フラグ = $subject\ of\ ICV$] であるパーツが複数存在する場合は、複数のパーツチェック値 $P-ICV_{ij}$ をパー

ツ番号順に連結したデータを対象にして8バイト単位で図37に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icv} を鍵とする）に入力して得た値として生成される。図37にコンテンツブロックのコンテンツチェック値 ICV_i を生成する構成例を示す。

【0287】

なお、フォーマット・タイプ2，3においては、ブロックのチェック値 ICV_i は定義されない。

【0288】

チェック値B： ICV_b は、ブロック情報鍵、コンテンツ鍵、ブロック情報全体に対するチェック値であり、例えば、前述の図24で説明した手法によって生成される。

【0289】

総チェック値 ICV_t は、前述のチェック値A： ICV_a 、チェック値B： ICV_b 、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 ICV_i 全体に対するチェック値であり、前述の図25で説明したようにチェック値A： ICV_a 等の各チェック値から生成される中間チェック値にシステム署名鍵 K_{sys} を適用して暗号化処理を実行することによって生成される。

【0290】

なお、フォーマット・タイプ2，3においては、総チェック値 ICV_t は、前述のチェック値A： ICV_a 、チェック値B： ICV_b にコンテンツデータ、すなわちブロック1のブロック鍵から最終ブロックまでのコンテンツデータ全体を連結したデータから生成される中間チェック値にシステム署名鍵 K_{sys} を適用して暗号化処理を実行することによって生成される。図38にフォーマット・タイプ2，3における総チェック値 ICV_t を生成する構成例を示す。

【0291】

固有チェック値 ICV_{dev} は、前述のローカリゼーションフラグが1にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV_t に置き換えられるチェック値であ

り、フォーマット・タイプ0, 1の場合は、前述のチェック値A: I C V a、チェック値B: I C V b、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値I C V i 全体に対するチェック値として生成される。具体的には、前述の図25、または図38で説明したようにチェック値A: I C V a等の各チェック値から生成される中間チェック値に記録再生器署名鍵K d e vを適用して暗号化処理を実行することによって生成される。

【0292】

次にフォーマットタイプ0~3各々における記録再生器300から記録デバイス400に対するコンテンツのダウンロード処理、および記録再生器300における記録デバイス400からの再生処理について図39~44のフローを用いて説明する。

【0293】

まず、フォーマットタイプ0, 1におけるコンテンツのダウンロード処理について図39を用いて説明する。

【0294】

図39に示す処理は、例えば図3に示す記録再生器300に記録デバイス400を装着することによって開始される。ステップS101は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図20の認証処理フローに従って実行される。

【0295】

ステップS101の認証処理が終了し、認証フラグがセットされると、記録再生器300は、ステップS102において、例えばコンテンツデータを格納したメディア500から、読み取り部304を介して所定のフォーマットに従ったデータを読み出すか、通信部305を使って通信手段600から所定のフォーマットに従ってデータを受信し、記録再生器300の制御部301が、データの内のヘッダ(Header)部分を記録再生器300の記録再生器暗号処理部302に送信する。

【0296】

次に、ステップS103において、暗号処理部302の制御部306が記録再

生器暗号処理部302の暗号／復号化部308にチェック値Aを計算させる。チェック値Aは、図23に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして図7を用いて説明したICV計算方法に従って計算される。次に、ステップS104において、チェック値Aとヘッダ(Header)内に格納されたチェック値:ICV aを比較し、一致していた場合にはステップS105へ進む。

【0297】

先に説明したようにチェック値A、ICV aは、識別情報、取扱方針の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値A生成鍵K i c v aを鍵とし、識別情報(Content ID)と取扱方針(Usage Policy)をメッセージとして、例えばICV計算方法に従って計算されるチェック値Aが、ヘッダ(Header)内に格納されたチェック値:ICV aと一致した場合には、識別情報、取扱方針の改竄はないと判断される。

【0298】

次に、ステップS105において、記録再生器暗号処理部302の制御部306は、配送鍵K d i sの取り出しまたは生成を記録再生器暗号処理部302の暗号／復号化部308に行わせる。配送鍵K d i sの生成方法は、先に説明した図22のステップS53と同様、例えば配送鍵用マスター鍵MK d i sを用いて行われる。

【0299】

次にステップS106において、記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号／復号化部308を使って、生成した配送鍵K d i sを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵K b i tとコンテンツ鍵K c o nの復号化処理を行う。

【0300】

さらに、ステップS107において、記録再生器暗号処理部302の制御部3

06は、記録再生器暗号処理部302の暗号／復号化部308において、復号化したブロック情報鍵K b i tでブロック情報を復号化する。

【0301】

さらに、ステップS108において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報（B I T）から、チェック値B（I C V b'）を生成する。チェック値Bは、図24に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報（B I T）からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ（Header）内のI C V bを比較し、一致していた場合にはステップS110へ進む。

【0302】

先に説明したように、チェック値B，I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値である。記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報（B I T）を8バイト単位に分割し排他的論理和して得られる値をDESで暗号化して生成したチェック値Bが、ヘッダ（Header）内に格納されたチェック値：I C V bと一致した場合には、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄はないと判断される。

【0303】

ステップS110において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に中間チェック値の計算をさせる。中間チェック値は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵K i c v tを鍵とし、検証したHeader内のチェック値A、チェック値B、保持しておいた全てのコンテンツチェック値をメッセージとして図7他で説明したI C V計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器300の記

録再生器暗号処理部 302 に保持しておく。

【0304】

次に、ステップ S111 において、記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 に総チェック値 $ICVt'$ の計算をさせる。総チェック値 $ICVt'$ は、図 25 に示すように、記録再生器暗号処理部 302 の内部メモリ 307 に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値を DES で暗号化して生成する。次に、ステップ S112 において、生成した総チェック値 $ICVt'$ とヘッダ (Header) 内の $ICVt$ を比較し、一致していた場合には、ステップ S113 へ進む。

【0305】

先に図 4 において説明したように、総チェック値 $ICVt$ は、 $ICVa$ 、 $ICVb$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成された総チェック値がヘッダ (Header) 内に格納されたチェック値： $ICVt$ と一致した場合には、 $ICVa$ 、 $ICVb$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【0306】

次に、ステップ S113 において、記録再生器 300 の制御部 301 は、ブロック情報 (BIT) 内のコンテンツブロック情報を取り出し、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。

【0307】

コンテンツブロックが検証対象になっていた場合には、ステップ S114 において、該当するコンテンツブロックを、記録再生器 300 の読み取り部 304 を使ってメディア 500 から読み出すか、記録再生器 300 の通信部 305 を使って通信手段 600 から受信し、記録再生器 300 の記録再生器暗号処理部 302 へ送信する。これを受信した記録再生器暗号処理部 302 の制御部 306 は、記録再生器暗号処理部 302 の暗号／復号化部 308 にコンテンツチェック値 $ICVi'$ を計算させる。

【0308】

コンテンツチェック値 ICV_i' は、先に説明したようにブロックが暗号化されている場合、コンテンツ鍵 K_{con} で、入力されたコンテンツブロックを DES の CBC モードで復号化し、その結果を全て 8 バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器 300 の内部メモリ 307 に格納されたコンテンツチェック値生成鍵 K_{icvc} で暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を 8 バイト単位で図 36 に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。

【0309】

次にステップ S115 において、記録再生器暗号処理部 302 の制御部 306 は、当該コンテンツチェック値と、ステップ S102 で記録再生器 300 の制御部 301 から受信したコンテンツブロック内の ICV を比較し、その結果を記録再生器 300 の制御部 301 に渡す。これを受信した記録再生器 300 の制御部 301 は、検証に成功していた場合、次の検証対象コンテンツブロックを取り出して記録再生器 300 の記録再生器暗号処理部 302 に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理を繰り返す（ステップ S116）。

【0310】

なお、ステップ S104、ステップ S109、ステップ S112、ステップ S115 のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとしてダウンロード処理は終了する。

【0311】

次に、ステップ S117 において、記録再生器 300 の記録再生器暗号処理部 302 は、ステップ S106 で復号化したブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を、記録再生器暗号処理部 302 の暗号／復号化部 308 に、相互認証の際に共有しておいたセッション鍵 K_{ses} で暗号化させる。記録再生器 300 の制御部 301 は、セッション鍵 K_{ses} で暗号化されたブロック情報鍵 K_{bit} とコンテンツ鍵 K_{con} を記録再生器 300 の記録再生器暗号処理部 302 から読み出し、これらのデータを記録再生器 300 の記録デバイスコントローラ

303を介して記録デバイス400に送信する。

【0312】

次に、ステップS118において、記録再生器300から送信されてきたブロック情報鍵Kbitとコンテンツ鍵Kconを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再び暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵Kstrで再暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconを読み出す。すなわち、配送鍵Kdisで暗号化されたブロック情報鍵Kbitとコンテンツ鍵Kconの鍵のかけかえを行なう。

【0313】

次に、ステップS119において、記録再生器300の制御部301は、データのヘッダ部の取扱方針 (Usage Policy) から利用制限情報を取り出し、ダウンロードしたコンテンツが当該記録再生器300のみで利用できるか否かの判定を行なう。この判定は、ローカリゼーションフラグ (利用制限情報) = 1 に設定されている場合は、ダウンロードしたコンテンツが当該記録再生器300のみで利用でき、ローカリゼーションフラグ (利用制限情報) = 0 に設定されている場合は、ダウンロードしたコンテンツが別の同様な記録再生器300でも利用できることを示す。判定の結果、ローカリゼーションフラグ (利用制限情報) = 1 であった場合には、ステップS120に進む。

【0314】

ステップS120において、記録再生器300の制御部301は、記録再生器固有のチェック値を記録再生器300の記録再生器暗号処理部302に計算させる。記録再生器固有のチェック値は、図25に示すように記録再生器暗号処理部302の内部メモリ307に保存されている記録再生器に固有の記録再生器署名鍵Kdevを鍵とし、ステップS110で生成した中間チェック値をDESで暗号化して生成する。計算された記録再生器固有のチェック値ICVdevは、総

チェック値 I C V t の代わりに上書きされる。

【0315】

先に説明したように、システム署名鍵 K s y s は、配信システムに共通の署名または I C V をつけるために使用するシステム署名鍵であり、また、記録再生器署名鍵 K d e v は、記録再生器毎に異なり、記録再生器が署名または I C V をつけるために使用する記録再生器署名鍵である。すなわち、システム署名鍵 K s y s によって署名されたデータは、同じシステム署名鍵を有するシステム（記録再生器）によってチェックが成功、すなわち総チェック値 I C V t が一致することになるので、共通に利用可能となるが、記録再生器署名鍵 K d e v を用いて署名された場合には、記録再生器署名鍵はその記録再生器に固有の鍵であるので、記録再生器署名鍵 K d e v を用いて署名されたデータ、すなわち、署名後、記録デバイスに格納されたデータは、他の記録再生器に、その記録デバイスを装置して再生しようとした場合、記録再生器固有のチェック値 I C V d e v が不一致となり、エラーとなるので再生できないことになる。本発明のデータ処理装置においては、利用制限情報の設定によって、システムに共通に使用できるコンテンツ、記録再生器固有に利用できるコンテンツを自在に設定できるものである。

【0316】

次に、ステップ S 1 2 1 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録再生器暗号処理部 3 0 2 に格納データフォーマットの形成を実行させる。先に説明したように、フォーマットタイプは 0 ～ 3 まで各タイプがあり、ヘッダ中の取扱方針（図 5 参照）中に設定され、この設定タイプにしたがって、先に説明した図 3 2 ～ 3 5 の右側の格納フォーマットにしたがってデータを形成する。この図 3 9 に示すフローはフォーマット 0, 1 のいずれかであるので、図 3 2, 3 3 のいずれかのフォーマットに形成される。

【0317】

ステップ S 1 2 1 において格納データフォーマットの形成が終了すると、ステップ 1 2 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、コンテンツを記録デバイス 4 0 0 の外部メモリ 4 0 2 に保存する。

【0318】

以上が、フォーマットタイプ0, 1におけるコンテンツデータのダウンロード処理の態様である。

【0319】

次に、フォーマットタイプ2におけるコンテンツデータのダウンロード処理について図40を用いて説明する。上記したフォーマットタイプ0, 1のダウンロード処理と異なる点を中心に説明する。

【0320】

ステップS101～S109は、上記したフォーマットタイプ0, 1のダウンロード処理と同様であるので説明は省略する。

【0321】

フォーマットタイプ2は、先に説明したようにコンテンツチェック値ICV_iが定義されていないので、ブロック情報中には、コンテンツチェック値ICV_iを持たない。フォーマットタイプ2における中間チェック値は、図38に示すようにチェック値A、チェック値Bと、第1ブロックの先頭データ（ブロック1のブロック鍵）から最終ブロックまでのコンテンツデータ全体を連結したデータに基づいて生成される中間チェック値にシステム署名鍵K_{sys}を適用して暗号化処理を実行することによって生成される。

【0322】

従って、フォーマットタイプ2のダウンロード処理においては、ステップS151においてコンテンツデータを読み出し、ステップS152において、チェック値A、チェック値Bと読み出したコンテンツデータに基づいて中間チェック値の生成を実行する。なお、コンテンツデータは暗号化されている場合でも、復号処理を行なわない。

【0323】

フォーマットタイプ2では、前述のフォーマットタイプ0, 1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となる。

【0324】

ステップS111以下の処理は、フォーマットタイプ0, 1における処理と同

様であるので説明を省略する。

【0325】

以上が、フォーマットタイプ2におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ2のダウンロード処理は、フォーマットタイプ0, 1での処理のようにブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

【0326】

次に、フォーマットタイプ3におけるコンテンツデータのダウンロード処理について図41を用いて説明する。上記したフォーマットタイプ0, 1, 2のダウンロード処理と異なる点を中心に説明する。

【0327】

ステップS101～S105は、上記したフォーマットタイプ0, 1, 2のダウンロード処理と同様であるので説明は省略する。

【0328】

フォーマットタイプ3は、基本的にフォーマットタイプ2における処理と共通する部分が多いが、フォーマットタイプ3はコンテンツ鍵を有しておらず、またブロック鍵Kb1cが記録デバイスにおいては保存鍵Kstrで暗号化されて格納される点がフォーマットタイプ2と異なる。

【0329】

フォーマットタイプ3のダウンロード処理におけるフォーマットタイプ2と相違する点を中心として説明する。フォーマットタイプ3では、ステップS105の次ステップであるステップS161において、ブロック情報鍵の復号を行なう。記録再生器暗号処理部302の制御部306が、記録再生器暗号処理部302の暗号／復号化部308を使って、ステップS105で生成した配送鍵Kdisを用いて、読み取り部304を介して受信したメディア500、または、通信部305を介して通信手段600から受信したデータのヘッダ部に格納されたブロック情報鍵Kbitの復号化処理を行う。フォーマットタイプ3では、データ中にコンテンツ鍵Kconが存在しないため、コンテンツ鍵Kconの復号化処理

は実行されない。

【0330】

次のステップS107では、ステップS161で復号したブロック情報鍵K b i tを用いてブロック情報の復号が実行され、さらに、ステップS162において、記録再生器暗号処理部302の制御部306は、ブロック情報鍵K b i t、およびブロック情報(B I T)から、チェック値B (I C V b') を生成する。チェック値Bは、記録再生器暗号処理部302の内部メモリ307に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i t、およびブロック情報(B I T)からなる排他的論理和値をDESで暗号化して生成する。次に、ステップS109において、チェック値Bとヘッダ(Header)内のI C V bを比較し、一致していた場合にはステップS151へ進む。

【0331】

フォーマットタイプ3では、チェック値B、I C V bは、ブロック情報鍵K b i t、ブロック情報の改竄を検証するためのチェック値として機能する。生成したチェック値Bが、ヘッダ(Header)内に格納されたチェック値:I C V bと一致した場合には、ブロック情報鍵K b i t、ブロック情報の改竄はないと判断される。

【0332】

ステップS151～S112は、フォーマットタイプ2の処理と同様であるので説明を省略する。

【0333】

ステップS163では、ステップS151で読み出したコンテンツデータに含まれるブロック鍵K b l cをステップS105で生成した配送鍵K d i sによって復号する。

【0334】

次にステップS164では、記録再生器300の記録再生器暗号処理部302が、ステップS161で復号化したブロック情報鍵K b i tと、ステップS163で復号したブロック鍵K b l cを、記録再生器暗号処理部302の暗号/復号化部308に、相互認証の際に共有しておいたセッション鍵K s e sで暗号化さ

せる。記録再生器300の制御部301は、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

【0335】

次に、ステップS165において、記録再生器300から送信されてきたブロック情報鍵K b i tとブロック鍵K b l cを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵K s e sで復号化させ、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵K s t rで再暗号化させ、記録再生器300の制御部301は、記録再生器300の記録デバイスコントローラ303を介し、記録デバイス400から保存鍵K s t rで再暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを読み出す。すなわち、当初、配送鍵K d i sで暗号化されたブロック情報鍵K b i tとブロック鍵K b l cを保存鍵K s t rで再暗号化されたブロック情報鍵K b i tとブロック鍵K b l cへ置き換えを行なう。

【0336】

以下のステップS119～S122は、前述のフォーマットタイプ0, 1, 2と同様であるので説明を省略する。

【0337】

以上が、フォーマットタイプ3におけるコンテンツデータのダウンロード処理の態様である。上述したようにフォーマットタイプ3のダウンロード処理は、フォーマットタイプ2と同様、ブロックデータの復号、コンテンツチェック値の照会処理を行なわないので、迅速な処理が可能となり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。また、ブロック鍵K b l cにより暗号化コンテンツを保護する範囲が局所化されているので、フォーマットタイプ2に比較して、よりセキュリティが高度となる。

【0338】

次に、フォーマットタイプ0～3各々における記録再生器300における記録

デバイス 4 0 0 からの再生処理について図 4 2 ～ 4 5 のフローを用いて説明する。

【 0 3 3 9 】

まず、フォーマットタイプ 0 におけるコンテンツの再生処理について図 4 2 を用いて説明する。

【 0 3 4 0 】

ステップ S 2 0 1 は、記録再生器と記録デバイス間における認証処理ステップであり、先に説明した図 2 0 の認証処理フローに従って実行される。

【 0 3 4 1 】

ステップ S 2 0 1 の認証処理が終了し、認証フラグがセットされると、記録再生器 3 0 0 は、ステップ S 2 0 2 において、記録デバイス 4 0 0 から所定のフォーマットに従ったデータのヘッダを読み出し、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に送信する。

【 0 3 4 2 】

次に、ステップ S 2 0 3 において、暗号処理部 3 0 2 の制御部 3 0 6 が記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 にチェック値 A を計算させる。チェック値 A は、先に説明した図 2 3 に示すように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されているチェック値 A 生成鍵 K i c v a を鍵とし、識別情報 (Content ID) と取扱方針 (Usage Policy) をメッセージとして計算される。次に、ステップ S 2 0 4 において、計算されたチェック値 A とヘッダ (Header) 内に格納されたチェック値 : I C V a を比較し、一致していた場合にはステップ S 2 0 5 へ進む。

【 0 3 4 3 】

チェック値 A, I C V a は、識別情報、取扱方針の改竄を検証するためのチェック値である。計算されたチェック値 A が、ヘッダ (Header) 内に格納されたチェック値 : I C V a と一致した場合には、記録デバイス 4 0 0 に格納された識別情報、取扱方針の改竄はないと判断される。

【 0 3 4 4 】

次に、ステップ S 2 0 5 において、記録再生器 3 0 0 の制御部 3 0 1 は、読み

出したヘッダから記録デバイス固有の保存鍵K s t rで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを取り出し、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介して記録デバイス4 0 0に送信する。

【0 3 4 5】

記録再生器3 0 0から送信されてきたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録デバイス4 0 0は、受信したデータを記録デバイス暗号処理部4 0 1の暗号／復号化部4 0 6に、記録デバイス暗号処理部4 0 1の内部メモリ4 0 5に保存してある記録デバイス固有の保存鍵K s t rで復号化处理させ、相互認証の際に共有しておいたセッション鍵K s e sで再び暗号化させる。この処理は、前述した（9）相互認証後の鍵交換処理の欄で詳しく述べた通りである。

【0 3 4 6】

ステップS 2 0 6では、記録再生器3 0 0の制御部3 0 1は、記録再生器3 0 0の記録デバイスコントローラ3 0 3を介し、記録デバイス4 0 0からセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信する。

【0 3 4 7】

次に、ステップS 2 0 7において、記録再生器3 0 0の制御部3 0 1は、受信したセッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを記録再生器3 0 0の記録再生器暗号処理部3 0 2に送信し、セッション鍵K s e sで再暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを受信した記録再生器3 0 0の記録再生器暗号処理部3 0 2は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8に、セッション鍵K s e sで暗号化されたブロック情報鍵K b i tとコンテンツ鍵K c o nを、相互認証の際に共有しておいたセッション鍵K s e sで復号化させる。

【0 3 4 8】

さらに、ステップS 2 0 8において、復号化したブロック情報鍵K b i tで、ステップS 2 0 2で読み出しておいたブロック情報を復号化する。なお、記録再生器3 0 0の記録再生器暗号処理部3 0 2は、復号化したブロック情報鍵K b i

t、コンテンツ鍵K c o nおよびブロック情報B I Tを、ステップS 2 0 2で読み出したヘッダに含まれるブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報B I Tに置き換えて保持しておく。また、記録再生器3 0 0の制御部3 0 1は、復号化されたブロック情報B I Tを記録再生器3 0 0の記録再生器暗号処理部3 0 2から読み出しておく。

【0349】

さらに、ステップS 2 0 9において、記録再生器暗号処理部3 0 2の制御部3 0 6は、ブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報（B I T）から、チェック値B（I C V b'）を生成する。チェック値Bは、図2 4に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されているチェック値B生成鍵K i c v bを鍵とし、ブロック情報鍵K b i t、コンテンツ鍵K c o nおよびブロック情報（B I T）からなる排他的論理和値をD E Sで暗号化して生成する。次に、ステップS 2 1 0において、チェック値Bとヘッダ（Header）内のI C V bを比較し、一致していた場合にはステップS 2 1 1へ進む。

【0350】

チェック値B、I C V bは、ブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄を検証するためのチェック値であり、生成したチェック値Bが、ヘッダ（Header）内に格納されたチェック値：I C V bと一致した場合には、記録デバイス4 0 0に保存されたデータ中のブロック情報鍵K b i t、コンテンツ鍵K c o n、ブロック情報の改竄はないと判断される。

【0351】

ステップS 2 1 1において、記録再生器暗号処理部3 0 2の制御部3 0 6は、記録再生器暗号処理部3 0 2の暗号／復号化部3 0 8に中間チェック値の計算をさせる。中間チェック値は、図2 5に示すように、記録再生器暗号処理部3 0 2の内部メモリ3 0 7に保存されている総チェック値生成鍵K i c v tを鍵とし、検証したHeader内のチェック値A、チェック値B、ブロック情報中の全てのコンテンツチェック値をメッセージとして図7他で説明したI C V計算方法に従って計算する。なお、生成した中間チェック値は、必要に応じて記録再生器3 0 0の

記録再生器暗号処理部 3 0 2 に保持しておく。

【 0 3 5 2 】

次に、ステップ S 2 1 2 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイス 4 0 0 の外部メモリ 4 0 2 から読み出したデータのヘッダ部に含まれる取扱方針 (Usage Policy) から利用制限情報を取り出し、再生予定のコンテンツが当該記録再生器 3 0 0 のみで利用できる (利用制限情報が 1) か、別の同様な記録再生器 3 0 0 でも利用できる (利用制限情報が 0) か判定する。判定の結果、利用制限情報が 1、すなわち再生コンテンツが当該記録再生器 3 0 0 のみで利用できる利用制限が設定されている場合には、ステップ S 2 1 3 に進み、利用制限情報が 0、すなわち別の同様な記録再生器 3 0 0 でも利用できる設定であった場合には、ステップ S 2 1 5 に進む。なお、ステップ S 2 1 2 の処理は暗号処理部 3 0 2 が行なってもよい。

【 0 3 5 3 】

ステップ S 2 1 3 では、記録再生器 3 0 0 の制御部 3 0 1 は、記録再生器固有のチェック値 $ICV_{dev'}$ を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に計算させる。記録再生器固有のチェック値 $ICV_{dev'}$ は、図 2 5 に示すように記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されている記録再生器署名鍵 K_{dev} を鍵とし、ステップ S 2 1 1 で保持しておいた中間チェック値を DES で暗号化して生成する。

【 0 3 5 4 】

次に、ステップ S 2 1 4 において、ステップ S 2 1 3 で計算した記録再生器固有のチェック値 $ICV_{dev'}$ とステップ S 2 0 2 で読み出したヘッダ内の ICV_{dev} を比較し、一致していた場合には、ステップ S 2 1 7 へ進む。

【 0 3 5 5 】

一方ステップ S 2 1 5 では、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に総チェック値 ICV_t の計算をさせる。総チェック値 ICV_t' は、図 2 5 に示すように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されているシステム署名鍵 K_{sys} を鍵とし、中間チェック値を DES で暗号化して生成する。次に、ステップ S 2 1

6において、生成した総チェック値 $ICVt'$ とヘッダ (Header) 内の $ICVt$ を比較し、一致していた場合には、ステップ S 2 1 7 へ進む。

【0356】

総チェック値 $ICVt$ 、および記録再生器固有のチェック値 $ICVdev$ は、 $ICVa$ 、 $ICVb$ 、各コンテンツブロックのチェック値全ての改竄を検証するためのチェック値である。従って、上述の処理によって生成されたチェック値がヘッダ (Header) 内に格納されたチェック値： $ICVt$ または $ICVdev$ と一致した場合には、記録デバイス 4 0 0 に格納された $ICVa$ 、 $ICVb$ 、各コンテンツブロックのチェック値全ての改竄はないと判断される。

【0357】

次に、ステップ S 2 1 7 において、記録再生器 3 0 0 の制御部 3 0 1 は、記録デバイス 4 0 0 からブロックデータを読み出す。さらに、ステップ S 2 1 8 において暗号化されているか否かを判定し、暗号化されている場合は、記録再生器 3 0 0 の暗号処理部 3 0 2 においてブロックデータの復号を行なう。暗号化されていない場合は、ステップ S 2 1 9 をスキップしてステップ S 2 2 0 に進む。

【0358】

次に、ステップ S 2 2 0 において、記録再生器 3 0 0 の制御部 3 0 1 は、ブロック情報 (BIT) 内のコンテンツブロック情報に基づいて、コンテンツブロックが検証対象になっているかいないか調べる。コンテンツブロックが検証対象になっている場合には、ヘッダ中のブロック情報中にコンテンツチェック値が格納されている。コンテンツブロックが検証対象になっていた場合には、ステップ S 2 2 1 において、該当するコンテンツブロックのコンテンツチェック値 $ICVi$ を計算させる。コンテンツブロックが検証対象になっていない場合には、ステップ S 2 2 1 と S 2 2 2 をスキップしてステップ S 2 2 3 に進む。

【0359】

コンテンツチェック値 $ICVi'$ は、先に図 3 6 で説明したようにブロックが暗号化されている場合、コンテンツ鍵 $Kcon$ で、入力されたコンテンツブロックを DES の CBC モードで復号化し、その結果を全て 8 バイト単位で排他的論理和して生成したコンテンツ中間値を記録再生器 3 0 0 の内部メモリ 3 0 7 に格

納されたコンテンツチェック値生成鍵 K_{icvc} で暗号化して生成する。また、ブロックが暗号化されていない場合は、データ（平文）全体を 8 バイト単位で図 3 6 に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵 K_{icvc} を鍵とする）に入力して得た値として生成される。

【0360】

ステップ S 2 2 2 においては、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、生成したコンテンツチェック値 $ICVi'$ と、ステップ S 2 0 2 で記録デバイス 4 0 0 から受信したヘッダ部に格納されたコンテンツチェック値 $ICVi$ とを比較し、その結果を記録再生器 3 0 0 の制御部 3 0 1 に渡す。これを受信した記録再生器 3 0 0 の制御部 3 0 1 は、検証に成功していた場合、ステップ S 2 2 3 において、記録再生器システム RAM 上に実行（再生）用コンテンツ平文データを格納する。記録再生器 3 0 0 の制御部 3 0 1 は、さらに次の検証対象コンテンツブロックを取り出して記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に検証させ、全てのコンテンツブロックを検証するまで同様の検証処理、RAM 格納処理を繰り返す（ステップ S 2 2 4）。

【0361】

なお、ステップ S 2 0 4、ステップ S 2 1 0、ステップ S 2 1 4、ステップ S 2 1 6、ステップ S 2 2 2 のいずれかにおいて、チェック値の一致が得られなかった場合はエラーとして再生処理は終了する。

【0362】

ステップ S 2 2 4 において全ブロック読み出しと判定されると、ステップ S 2 2 5 に進み、コンテンツ（プログラム、データ）の実行、再生が開始される。

【0363】

以上が、フォーマットタイプ 0 におけるコンテンツデータの再生処理の態様である。

【0364】

次に、フォーマットタイプ 1 におけるコンテンツデータの再生処理について図 4 3 を用いて説明する。上記したフォーマットタイプ 0 の再生処理と異なる点を中心に説明する。

【0365】

ステップS201～ステップS217までの処理は、上記したフォーマットタイプ0の再生処理と同様であるので説明は省略する。

【0366】

フォーマットタイプ1では、ステップS231において、暗号化パーツの復号が実行され、パーツICVが生成される。さらに、ステップS232において、ブロックICVi' が生成される。先に説明したように、フォーマット・タイプ1においては、ブロック内のパーツのうち少なくとも1つがチェック値ICViの対象データである場合は、そのブロックに関してコンテンツチェック値ICViが定義される。ブロックiにおけるパーツjのチェック値P-ICVijは、パーツjが暗号化されている場合、平文（復号文）全体を8バイト単位で排他論理和した値をコンテンツチェック値生成鍵Kicvcで暗号化した値として生成される。また、パーツjが暗号化されていない場合は、データ（平文）全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵Kicvcを鍵とする）に入力して得た値として生成される。

【0367】

さらに、1つのブロックi内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが1つのみ存在する場合は、上述の手法で生成したチェック値P-ICVijをそのままブロックのチェック値ICViとし、また、1つのブロックi内にチェック対象であることを示す[ICVフラグ=subject of ICV]であるパーツが複数存在する場合は、複数のパーツチェック値P-ICVijをパーツ番号順に連結したデータを対象にしてデータ（平文）全体を8バイト単位で図36に示す改竄チェック値生成関数（DES-CBC-MAC、コンテンツチェック値生成鍵Kicvcを鍵とする）に入力して得た値として生成される。これは、先に図37で説明した通りである。

【0368】

フォーマットタイプ1では、上述の手順で生成されたコンテンツチェック値の

比較処理がステップ S 2 2 2 で実行されることになる。以下のステップ S 2 2 3 以下の処理はフォーマットタイプ 0 と同様であるので説明は省略する。

【 0 3 6 9 】

次に、フォーマットタイプ 2 におけるコンテンツデータの再生処理について図 4 4 を用いて説明する。上記したフォーマットタイプ 0, 1 の再生処理と異なる点を中心に説明する。

【 0 3 7 0 】

ステップ S 2 0 1 ~ S 2 1 0 は、上記したフォーマットタイプ 0, 1 の再生処理と同様であるので説明は省略する。

【 0 3 7 1 】

フォーマットタイプ 2 においては、フォーマットタイプ 0, 1 において実行されたステップ S 2 1 1 ~ S 2 1 6 の処理が実行されない。また、フォーマットタイプ 2 においては、コンテンツチェック値を持たないため、フォーマットタイプ 0, 1 において実行されたステップ S 2 2 2 のコンテンツチェック値の検証も実行されない。

【 0 3 7 2 】

フォーマットタイプ 2 のデータ再生処理においては、ステップ S 2 1 0 のチェック値 B の検証ステップの後、ステップ S 2 1 7 に進み、記録再生器 3 0 0 の制御部 3 0 1 の制御によって、ブロックデータが読み出される。さらに、ステップ S 2 4 1 において、記録再生器 3 0 0 の暗号処理部 3 0 6 によるブロックデータに含まれるブロック鍵 K b 1 c の復号処理が実行される。記録デバイス 4 0 0 に格納されたブロック鍵 K b 1 c は、図 3 4 で示すようにコンテンツ鍵 K c o n で暗号化されており、先のステップ S 2 0 7 において復号したコンテンツ鍵 K c o n を用いてブロック鍵 K b 1 c の復号を行なう。

【 0 3 7 3 】

次に、ステップ S 2 4 2 において、ステップ S 2 4 1 で復号されたブロック鍵 K b 1 c を用いてブロックデータの復号処理が実行される。さらに、ステップ S 2 4 3 において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップ S 2 1 7 ~ ステップ S 2 4 3 の処理が全ブロックについて繰り返

し実行される。ステップS 2 4 4において全ブロック読み出しと判定されると再生処理は終了する。

【0 3 7 4】

このようにフォーマットタイプ2の処理は、総チェック値等のチェック値検証処理を省略しており、高速な復号処理の実行に適している構成であり、音楽データ等リアルタイム処理が要求されるデータ処理に適したフォーマットである。

【0 3 7 5】

次にフォーマットタイプ3におけるコンテンツデータの再生処理について図45を用いて説明する。上記したフォーマットタイプ0, 1, 2の再生処理と異なる点を中心に説明する。

【0 3 7 6】

フォーマットタイプ3は、基本的にフォーマットタイプ2における処理と共通する部分が多いが、フォーマットタイプ3は図35において説明したようにコンテンツ鍵を有しておらず、またブロック鍵K b l cが記録デバイスにおいては保存鍵K s t rで暗号化されて格納される点がフォーマットタイプ2と異なる。

【0 3 7 7】

ステップS 2 0 1～S 2 1 0において、ステップS 2 5 1、ステップS 2 5 2、ステップS 2 5 3、ステップS 2 5 4の処理は、前述のフォーマットタイプ0, 1, 2における対応処理と異なりコンテンツ鍵を含まない処理として構成されている。

【0 3 7 8】

ステップS 2 5 1において、記録再生器300の制御部301は、読み出したヘッダから記録デバイス固有の保存鍵K s t rで暗号化されたブロック情報鍵K b i tを取り出し、記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

【0 3 7 9】

記録再生器300から送信されてきたブロック情報鍵K b i tを受信した記録デバイス400は、受信したデータを記録デバイス暗号処理部401の暗号／復

号化部 4 0 6 に、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K_{str} で復号化处理させ、相互認証の際に共有しておいたセッション鍵 K_{ses} で再暗号化させる。この処理は、前述した (9) 相互認証後の鍵交換処理の欄で詳しく述べた通りである。

【0380】

ステップ S 2 5 2 では、記録再生器 3 0 0 の制御部 3 0 1 は、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介し、記録デバイス 4 0 0 からセッション鍵 K_{ses} で再暗号化されたブロック情報鍵 K_{bit} を受信する。

【0381】

次に、ステップ S 2 5 3 において、記録再生器 3 0 0 の制御部 3 0 1 は、受信したセッション鍵 K_{ses} で再暗号化されたブロック情報鍵 K_{bit} を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 に送信し、セッション鍵 K_{ses} で再暗号化されたブロック情報鍵 K_{bit} を受信した記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 に、セッション鍵 K_{ses} で暗号化されたブロック情報鍵 K_{bit} を、相互認証の際に共有しておいたセッション鍵 K_{ses} で復号化させる。

【0382】

さらに、ステップ S 2 0 8 において、復号化したブロック情報鍵 K_{bit} で、ステップ S 2 0 2 で読み出しておいたブロック情報を復号化する。なお、記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 は、復号化したブロック情報鍵 K_{bit} およびブロック情報 BIT を、ステップ S 2 0 2 で読み出したヘッダに含まれるブロック情報鍵 K_{bit} およびブロック情報 BIT に置き換えて保持しておく。また、記録再生器 3 0 0 の制御部 3 0 1 は、復号化されたブロック情報 BIT を記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 から読み出しておく。

【0383】

さらに、ステップ S 2 5 4 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、ブロック情報鍵 K_{bit} およびブロック情報 (BIT) から、チェック値 $B (ICVb')$ を生成する。チェック値 B は、図 2 4 に示すように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 に保存されているチェック値 B 生成鍵

K i c v b を鍵とし、ブロック情報鍵 K b i t およびブロック情報 (B I T) からなる排他的論理和値を D E S で暗号化して生成する。次に、ステップ S 2 1 0 において、チェック値 B とヘッダ (Header) 内の I C V b を比較し、一致していた場合にはステップ S 2 1 1 へ進む。

【 0 3 8 4 】

フォーマットタイプ 3 では、さらに、ブロック鍵が記録デバイスでの格納時に保存鍵によって暗号化されるため、記録デバイス 4 0 0 における保存鍵での復号処理、およびセッション鍵での暗号化処理、さらに、記録再生器 3 0 0 でのセッション鍵での復号処理が必要となる。これらの一連の処理がステップ S 2 5 5、ステップ S 2 5 6 で示した処理ステップである。

【 0 3 8 5 】

ステップ S 2 5 5 では、記録再生器 3 0 0 の制御部 3 0 1 は、ステップ S 2 1 7 で読み出したブロックから記録デバイス固有の保存鍵 K s t r で暗号化されたブロック鍵 K b l c を取り出し、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。

【 0 3 8 6 】

記録再生器 3 0 0 から送信されてきたブロック鍵 K b l c を受信した記録デバイス 4 0 0 は、受信したデータを記録デバイス暗号処理部 4 0 1 の暗号／復号化部 4 0 6 に、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K s t r で復号化処理させ、相互認証の際に共有しておいたセッション鍵 K s e s で再暗号化させる。この処理は、前述した「(9) 相互認証後の鍵交換処理」の欄で詳しく述べた通りである。

【 0 3 8 7 】

ステップ S 2 5 6 では、記録再生器 3 0 0 の制御部 3 0 1 は、記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介し、記録デバイス 4 0 0 からセッション鍵 K s e s で再暗号化されたブロック鍵 K b l c を受信する。

【 0 3 8 8 】

次に、ステップ S 2 5 7 において、記録再生器 3 0 0 の暗号処理部 3 0 6 によるブロック鍵 K b l c のセッション鍵 K s e s を用いた復号処理が実行される。

【0389】

次に、ステップS242において、ステップS257で復号されたブロック鍵Kb1cを用いてブロックデータの復号処理が実行される。さらに、ステップS243において、コンテンツ（プログラム、データ）の実行、再生処理が実行される。ステップS217～ステップS243の処理が全ブロックについて繰り返し実行される。ステップS244において全ブロック読み出しと判定されると再生処理は終了する。

【0390】

以上の処理が、フォーマットタイプ3におけるコンテンツの再生処理である。総チェック値の検証処理が省略された点でフォーマットタイプ2と類似するが、ブロック鍵の鍵交換処理を含む点でフォーマットタイプ2に比較して、さらにセキュリティ・レベルの高い処理構成となっている。

【0391】

(11) コンテンツプロバイダにおけるチェック値(ICV)生成処理態様

上述の実施例中において、各種のチェック値ICVについての検証処理が、コンテンツのダウンロード、または再生処理等の段階で実行されることを説明してきた。ここでは、これら各チェック値(ICV)生成処理、検証処理の態様について説明する。

【0392】

まず、実施例で説明した各チェック値について、簡潔にまとめると、本発明のデータ処理装置において利用されるチェック値ICVには以下のものがある。

【0393】

チェック値A, ICVa: コンテンツデータ中の識別情報、取扱方針の改竄を検証するためのチェック値。

チェック値B, ICVb: ブロック情報鍵Kbit、コンテンツ鍵Kcon、ブロック情報の改竄を検証するためのチェック値。

コンテンツチェック値ICVi: コンテンツの各コンテンツブロックの改竄を検証するためのチェック値。

総チェック値ICVt: チェック値ICVa、チェック値ICVb、各コンテ

ンツブロックのチェック値全ての改竄を検証するためのチェック値である。

再生器固有チェック値 ICV_{dev} : ローカリゼーションフラグが1にセットされている場合、すなわち、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV_t に置き換えられるチェック値であり、前述のチェック値A : ICV_a 、チェック値B : ICV_b 、さらにコンテンツのチェック対象となっている各ブロックに含まれるチェック値 ICV_i 全体に対するチェック値として生成される。

フォーマットによっては、 ICV_t 、 ICV_{dev} がチェックする対象に含まれるのは、各コンテンツブロックのチェック値ではなく、コンテンツそのものとなる場合もある。

【0394】

以上の各チェック値が本発明のデータ処理装置において用いられる。上記各チェック値の中で、チェック値A、チェック値B、総チェック値、コンテンツチェック値は、例えば図32～35、および図6に示されるようにコンテンツデータを提供するコンテンツプロバイダ、あるいはコンテンツ管理者によって、それぞれの検証対象データに基づいて ICV 値が生成され、コンテンツと共にデータ中に格納されて記録再生器300の利用者に提供される。記録再生器の利用者、すなわちコンテンツ利用者は、このコンテンツを記録デバイスにダウンロードする際、または再生する際にそれぞれの検証対象データに基づいて検証用の ICV を生成して、格納済みの ICV との比較を行なう。また、再生器固有チェック値 ICV_{dev} は、コンテンツが記録再生器固有に利用可能であることを示している場合に、総チェック値 ICV_t に置き換えられて、記録デバイスに格納されるものである。

【0395】

チェック値の生成処理は、前述の実施例中では、主としてDES-CBCによる生成処理構成を説明してきた。しかし、 ICV の生成処理態様には、上述の方法に限らず様々な生成処理態様、さらに、様々な検証処理態様がある。特にコンテンツ提供者または管理者と、コンテンツ利用者との関係においては、以下に説明する各種の ICV 生成および検証処理構成が可能である。

【 0 3 9 6 】

図 4 6 ～ 図 4 8 にチェック値 I C V の生成者における生成処理と、検証者による検証処理を説明する図を示す。

【 0 3 9 7 】

図 4 6 は、上述の実施例中で説明した D E S - C B C による I C V の生成処理を、例えばコンテンツ提供者または管理者である I C V 生成者が行ない、生成した I C V をコンテンツと共に記録再生器利用者、すなわち検証者に提供する構成である。この場合に記録再生器利用者、すなわち検証者が検証処理の際に必要な鍵は、例えば図 1 8 に示す内部メモリ 3 0 7 に格納された各チェック値生成鍵である。コンテンツ利用者である検証者（記録再生器利用者）は、内部メモリ 3 0 7 に格納されたチェック値生成鍵を使用して、検証対象のデータに D E S - C B C を適用してチェック値を生成して格納チェック値と比較処理を実行する。この場合、各チェック値生成鍵は、I C V の生成者と、検証者が秘密に共有する鍵として構成される。

【 0 3 9 8 】

図 4 7 は、コンテンツ提供者または管理者である I C V の生成者が公開鍵暗号系のデジタル署名により I C V を生成して、生成した I C V をコンテンツと共にコンテンツ利用者、すなわち検証者に提供する。コンテンツ利用者、すなわち検証者は、I C V 生成者の公開鍵を保存し、この公開鍵を用いて I C V の検証処理を実行する構成である。この場合、コンテンツ利用者（記録再生器利用者）、すなわち検証者の有する I C V 生成者の公開鍵は秘密にする必要がなく、管理は容易となる。I C V の生成、管理が 1 つのエンティティにおいて実行される場合等、I C V の生成、管理が高いセキュリティ管理レベルで行われている場合に適した態様である。

【 0 3 9 9 】

図 4 8 は、コンテンツ提供者または管理者である I C V の生成者が公開鍵暗号系のデジタル署名により I C V を生成して、生成した I C V をコンテンツと共にコンテンツ利用者、すなわち検証者に提供し、さらに、検証者が検証に用いる公開鍵を公開鍵証明書（例えば図 1 4 参照）に格納してコンテンツデータと共に記

録再生器利用者、すなわち検証者に提供する。ICVの生成者が複数存在する場合には、各生成者は、公開鍵の正当性を証明するデータ（公開鍵証明書）を鍵管理センタに作成してもらう。

【0400】

ICVの検証者であるコンテンツ利用者は、鍵管理センタの公開鍵を持ち、検証者は公開鍵証明書の検証を鍵管理センタの公開鍵によって実行し、正当性が確認されたら、その公開鍵証明書に格納されたICVの生成者の公開鍵を取り出す。さらに、取り出したICVの生成者の公開鍵を用いてICVの検証を実行する。

【0401】

この方法は、ICVの生成者が複数あり、それらの管理を実行するセンタによる管理の実行システムが確立している場合に有効な態様である。

【0402】

(12) マスタ鍵に基づく暗号処理鍵生成構成

次に、本発明のデータ処理システムにおける特徴的な構成の1つである、マスタ鍵に基づく各種暗号処理用鍵の生成構成について説明する。

【0403】

先に図18を用いて説明したように、本発明のデータ処理装置における記録再生器300の内部メモリには、様々なマスタ鍵が格納され、これらの各マスタ鍵を用いて、例えば認証鍵Kakeを生成（数3参照）したり、あるいは配送鍵Kdisを生成（数4参照）する構成となっている。

【0404】

従来、1対1のエンティティ間、すなわちコンテンツプロバイダとコンテンツ利用者間、あるいは、上述の本発明のデータ処理装置における記録再生器300と記録メディア400との間において暗号通信、相互認証、MAC生成、検証等を行なう際には、各エンティティに共通な秘密情報、例えば鍵情報を保持させていた。また、1対多の関係、例えば1つのコンテンツプロバイダに対する多数のコンテンツ利用者、あるいは1つの記録再生器に対する多数の記録メディア等の関係においては、すべてのエンティティ、すなわち多数のコンテンツ利用者、あ

るいは多数の記録メディアにおいて共有させた秘密情報、例えば鍵情報を格納保持させる構成とするか、あるいは、1つのコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報(e x. 鍵)を個別に管理し、これを各コンテンツ利用者に応じて使い分けていた。

【0405】

しかしながら、上記のような1対多の利用関係がある場合、すべてが共有する秘密情報(e x. 鍵)を所有する構成においては、1箇所の秘密漏洩が発生すると同じ秘密情報(e x. 鍵)を利用している者すべてに影響が及ぶという欠点がある。また、1つの管理者、例えばコンテンツプロバイダが多数のコンテンツ利用者各々の秘密情報(e x. 鍵)を個別に管理し、これを各コンテンツ利用者に応じて使い分ける構成とすると、すべての利用者を識別し、かつその識別データに固有の秘密情報(e x. 鍵)を対応づけたリストが必要となり、利用者の増大に伴うリストの保守管理の負担が増加するという欠点がある。

【0406】

本発明のデータ処理装置においては、このようなエンティティ間における秘密情報の共有における従来の問題点をマスター鍵の保有、およびマスター鍵から各種の個別鍵を生成する構成により解決した。以下、この構成について説明する。

【0407】

本発明のデータ処理装置においては、記録デバイスやコンテンツを格納したメディア、または記録再生器間での各種の暗号処理、認証処理等において異なる個別の鍵が必要になる場合、その個別の鍵を、デバイスやメディアが固有に持つ識別子データ(ID)などの個別情報と記録再生器300内であらかじめ決められた個別鍵生成方式を用いて生成する。この構成により万が一、生成された個別の鍵が特定された場合でもマスター鍵の漏洩を防止すれば、システム全体への被害を防ぐことが可能となる。またマスター鍵によって鍵を生成する構成により対応づけリストの管理も不要となる。

【0408】

具体的な構成例について、図を用いて説明する。まず、図49に各種の鍵を記録再生器300の有する各種のマスター鍵を用いて生成する構成を説明する図を示

す。図49のメディア500、通信手段600からは、すでに説明した実施例と同様、コンテンツが入力される。コンテンツはコンテンツ鍵 K_{con} によって暗号化され、またコンテンツ鍵 K_{con} は、配送鍵 K_{dis} によって暗号化されている。

【0409】

例えば、記録再生器300がメディア500、通信手段600からコンテンツを取り出して、記録デバイス400にダウンロードしようとする場合、先の図22、図39～41において説明したように、記録再生器300は、コンテンツ鍵を暗号化している配送鍵 K_{dis} を取得することが必要となる。この K_{dis} をメディア500、通信手段600から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、このような鍵の多数のユーザに対する配布構成は、先にも説明したようにシステム全体に影響を及ぼす漏洩の可能性がある。

【0410】

本発明のデータ処理システムでは、この配送鍵 K_{dis} を図49の下部に示すように、記録再生器300のメモリに格納された配送鍵用マスター鍵 MK_{dis} と、コンテンツIDに基づく処理、すなわち $K_{dis} = DES(MK_{dis}, \text{コンテンツID})$ を適用して配送鍵 K_{dis} を生成する構成としている。本構成によれば、メディア500、通信手段600からコンテンツを供給するコンテンツプロバイダとそのコンテンツ利用者である記録再生器300間におけるコンテンツ配布構成において、コンテンツプロバイダが多数存在した場合であっても、個々の配送鍵 K_{dis} をメディア、通信媒体等を介して流通させる必要もなく、また、各記録再生器300に格納する必要もなく、セキュリティを高度に保つことが可能となる。

【0411】

次に、認証鍵 K_{ake} の生成について説明する。先に説明した図22、図39～41の記録再生器300から記録メディア400に対するダウンロード処理、あるいは図28、図42～45で説明した記録メディア400に格納されたコンテンツを記録再生器300において実行、再生する場合、記録再生器300と記

録メディア400間における相互認証処理（図20参照）が必要となる。

【0412】

図20で説明したように、この認証処理において記録再生器300は認証鍵Kakeが必要となる。記録再生器300は、認証鍵を例えば記録メディア400から直接取得したり、あるいは予め記録再生器300が取得して記録再生器300内のメモリに格納しておくことも可能であるが、上述の配送鍵の構成と同様、このような鍵の多数のユーザに対する配布構成は、システム全体に影響を及ぼす漏洩の可能性がある。

【0413】

本発明のデータ処理システムでは、この認証鍵Kakeを図49の下部に示すように、記録再生器300のメモリに格納された認証鍵用マスター鍵MKakeと、記録デバイス識別ID: IDmemに基づく処理、すなわち $Kake = DES(MKake, IDmem)$ によって認証鍵Kakeを求める構成としている。

【0414】

さらに、図22、図39～41の記録再生器300から記録メディア400に対するダウンロード処理、あるいは図28、図42～45で説明した記録メディア400に格納されたコンテンツを記録再生器300において実行、再生する場合、記録再生器固有に利用可能なコンテンツである場合の記録再生器固有チェック値ICVdevの生成処理に必要な記録再生器署名鍵Kdevについても上述の配送鍵、認証鍵と同様の構成とすることができる。上述の実施例中では、記録再生器署名鍵Kdevは内部メモリに格納する構成としていたが、記録再生器署名鍵用マスター鍵MKdevをメモリに格納し、記録再生器署名鍵Kdevは内部メモリに格納せず、必要に応じて図49の下部に示すように記録再生器識別子: IDdevと記録再生器署名鍵用マスター鍵MKdevに基づいて、 $Kdev = DES(MKdev, IDdev)$ によって記録再生器署名鍵Kdevを求める構成とすることで、記録再生器署名鍵Kdevを機器個別に持たせる必要がなくなるという利点が挙げられる。

【0415】

このように、本発明のデータ処理装置においては、プロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各IDから逐次的に生成する構成としたので、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

【0416】

本構成に関する複数の処理例についてフローを示して説明する。図50は、コンテンツ製作または管理者におけるマスター鍵を用いたコンテンツ等の暗号化処理と、ユーザデバイス、例えば上述の実施例における記録再生器300におけるマスター鍵を用いた暗号化データの復号処理例である。

【0417】

コンテンツ製作または管理者におけるステップS501は、コンテンツに対する識別子（コンテンツID）を付与するステップである。ステップS502は、コンテンツ製作または管理者の有するマスター鍵とコンテンツIDとに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 K_{dis} を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{コンテンツID})$ によって配送鍵 K_{dis} を生成する。次に、ステップS503は、コンテンツの一部、または全部を鍵（例えば配送鍵 K_{dis} ）によって暗号化するステップである。コンテンツ製作者は、このようなステップを経て暗号化処理を行なったコンテンツをDVD等のメディア、通信手段等を介して配信する。

【0418】

一方、例えば記録再生器300等のユーザデバイス側では、ステップS504において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツIDを読み出す。次に、ステップS505において、読み出したコンテンツIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{dis} を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, \text{コンテンツID})$ となる。ステップS506で、この鍵を用いてコンテンツを復号し、ステップS507で復号コンテンツ

の利用、すなわち再生またはプログラムを実行する。

【0419】

この例においては、図50下段に示すように、コンテンツ製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵MKdis）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID（コンテンツID）に基づいて生成する。

【0420】

このシステムでは、万が一配送鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、コンテンツIDの異なる他のコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

【0421】

次に図5.1を用いて、コンテンツ製作または管理者が複数のマスター鍵を所有して、コンテンツの配信対象に応じた処理を実行する例について説明する。

【0422】

コンテンツ製作または管理者におけるステップS511は、コンテンツに対する識別子（コンテンツID）を付与するステップである。ステップS512は、コンテンツ製作または管理者の有する複数のマスター鍵（例えば複数の配送鍵生成用マスター鍵MKdis）から1つのマスター鍵を選択するステップである。この選択処理は図52を用いてさらに説明するが、コンテンツの利用者の国ごと、機種ごと、あるいは機種のバージョンごとなどに対応付けて予め適用するマスター鍵を設定しておき、その設定に従って実行するものである。

【0423】

次に、ステップS513では、ステップS512で選択したマスター鍵と、ステップS511で決定したコンテンツIDとに基づいて暗号化用の鍵を生成する。これは例えば、配送鍵Kdisiを生成する工程とすれば、 $Kdisi = DES(MKdisi, \text{コンテンツID})$ によって生成する。次に、ステップS51

4 はコンテンツの一部、または全部を鍵（例えば配送鍵 K_{disi} ）によって暗号化するステップである。コンテンツ製作者は、ステップ S515 において、コンテンツ ID と、使用したマスター鍵識別情報と、暗号化コンテンツを 1 つの配布単位として暗号化処理を行なったコンテンツを DVD 等のメディア、通信手段等を介して配信する。

【0424】

一方、例えば記録再生器 300 等のユーザデバイス側では、ステップ S516 において、DVD 等のメディア、通信手段等を介して配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有するか否かについて判定する。コンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を持たない場合は、その配布コンテンツは、そのユーザデバイスにおいては利用できないものであり、処理は終了する。

【0425】

配信されたコンテンツデータ中のマスター鍵識別情報に対応するマスター鍵を自己が所有する場合は、ステップ S517 において、メディア、通信手段等を介して受領したコンテンツデータ中からコンテンツ ID を読み出す。次に、ステップ S518 において、読み出したコンテンツ ID と所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{disi} を得るものである場合は、例えば配送鍵 $K_{disi} = DES(MK_{disi}, \text{コンテンツ ID})$ となる。ステップ S519 で、この鍵を用いてコンテンツを復号し、ステップ S520 で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

【0426】

この例においては、図 51 下段に示すように、コンテンツ製作または管理者は、複数のマスター鍵、例えば複数の配送鍵生成用マスター鍵 $MK_{dis1} \sim n$ からなるマスター鍵セットを有する。一方、ユーザデバイスには 1 つのマスター鍵例えば 1 つの配送鍵生成用マスター鍵 KK_{disi} を有し、コンテンツ製作または管理者が MK_{disi} を用いて暗号化処理している場合のみ、ユーザデバイスは、そのコンテンツを復号して利用することができる。

【0427】

この図51のフローに示す態様の具体例として、国毎に異なるマスター鍵を適用した例を図52に示す。コンテンツプロバイダは、マスター鍵MK1～nを有し、MK1は日本向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いる。例えば、コンテンツIDとMK1から暗号化鍵K1を生成してK1によってコンテンツを暗号化する。また、MK2はUS向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用い、MK3はEU（ヨーロッパ）向けのユーザデバイスに配信するコンテンツの暗号化処理を実行する鍵生成に用いるよう設定している。

【0428】

一方、日本向けユーザデバイス、具体的には日本で販売されるPCまたはゲーム機器等の記録再生器には、マスター鍵MK1がその内部メモリに格納され、US向けユーザデバイスには、マスター鍵MK2がその内部メモリに格納され、EU向けユーザデバイスには、マスター鍵MK3がその内部メモリに格納されている。

【0429】

このような構成において、コンテンツプロバイダは、コンテンツを利用可能なユーザデバイスに応じて、マスター鍵MK1～nから、マスター鍵を選択的に使用してユーザデバイスに配信するコンテンツの暗号化処理を実行する。例えばコンテンツを日本向けのユーザデバイスのみ利用可能とするためには、マスター鍵MK1を用いて生成された鍵K1によってコンテンツを暗号化する。この暗号化コンテンツは、日本向けユーザデバイスに格納されたマスター鍵MK1を用いて復号可能、すなわち復号鍵を生成可能であるが、他のUS、またはEU向けのユーザデバイスに格納されたマスター鍵MK2、MK3からは鍵K1を得ることができないので、暗号化コンテンツの復号は不可能となる。

【0430】

このように、コンテンツプロバイダが複数のマスター鍵を選択的に使用することにより、様々なコンテンツの利用制限を設定することができる。図52では、ユーザデバイスの国別にマスター鍵を区別する例を示したが、前述のように、ユ

ーザデバイスの機種に応じて、あるいはバージョンに応じてマスター鍵を切り換える等、様々な利用形態が可能である。

【0431】

次に、図53にメディア固有の識別子、すなわちメディアIDとマスター鍵を組み合わせた処理例を示す。ここで、メディアとは例えばDVD、CD等のコンテンツを格納したメディアである。メディアIDは、1つ1つのメディアごとに固有としてもよいし、たとえば、映画などのコンテンツのタイトルごとに固有としてもよいし、メディアの製造ロットごとに固有としてもよい。このようにメディアIDの割り当て方法としては様々な方法を用いることができる。

【0432】

メディア製作または管理者におけるステップS521は、メディアに対する識別子（メディアID）を決定するステップである。ステップS522は、メディア製作または管理者の有するマスター鍵とメディアIDとに基づいてメディア内の格納コンテンツ等を暗号化する鍵を生成するステップである。これは例えば、配送鍵 K_{dis} を生成する工程とすれば、前述の $K_{dis} = DES(MK_{dis}, \text{メディアID})$ によって配送鍵 K_{dis} を生成する。次に、ステップS523は、メディア格納コンテンツの一部、または全部を鍵（例えば配送鍵 K_{dis} ）によって暗号化するステップである。メディア製作者は、このようなステップを経て暗号化処理を行なったコンテンツ格納メディアを供給する。

【0433】

一方、例えば記録再生器300等のユーザデバイス側では、ステップS524において、供給されたメディアからメディアIDを読み出す。次に、ステップS525において、読み出したメディアIDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、配送鍵 K_{dis} を得るものである場合は、例えば配送鍵 $K_{dis} = DES(MK_{dis}, \text{メディアID})$ となる。ステップS526で、この鍵を用いてコンテンツを復号し、ステップS527で復号コンテンツの利用、すなわち再生またはプログラムを実行する。

【0434】

この例においては、図 5 3 下段に示すように、メディア製作または管理者と、ユーザデバイスの双方がマスター鍵（例えば配送鍵生成用マスター鍵 MK_{dis} ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各 ID（メディア ID）に基づいて生成する。

【0 4 3 5】

このシステムでは、万が一メディア鍵が第三者に漏洩した場合、そのメディア内のコンテンツの復号が第三者において可能となるが、メディア ID の異なる他のメディアに格納されたコンテンツの復号は防止することが可能であるため、1 つのメディア鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、ユーザデバイス側、すなわち記録再生器において、メディア毎の鍵の対応付けリストを保持する必要がないという効果もある。また、1 つのメディア鍵で暗号化されるコンテンツサイズは、そのメディア内に格納可能な容量に制限されるため、暗号文攻撃のために必要な情報量に達する可能性は少なく、暗号解読の可能性を低減させることができる。

【0 4 3 6】

次に、図 5 4 に記録再生器固有の識別子、すなわち記録再生器 ID とマスター鍵を組み合わせた処理例を示す。

【0 4 3 7】

記録再生器利用者におけるステップ S 5 3 1 は、記録再生器の例えば内部メモリに格納されたマスター鍵と記録再生器 ID とに基づいてコンテンツ等を暗号化する鍵を生成するステップである。これは例えば、コンテンツ鍵 K_{con} を生成する工程とすれば、 $K_{con} = DES(MK_{con}, \text{記録再生器 ID})$ によってコンテンツ鍵 K_{con} を生成する。次に、ステップ S 5 3 2 は、格納するコンテンツの一部、または全部を鍵（例えば配送鍵 K_{con} ）によって暗号化するステップである。ステップ S 5 3 3 は、暗号化コンテンツを例えばハードディスク等の記録デバイスに格納する。

【0 4 3 8】

一方、記録再生器を管理するシステム管理者側では、コンテンツを格納した記録再生器利用者から格納データの復旧を依頼されると、ステップ S 5 3 4 におい

て、記録再生器から、記録再生器IDを読み出す。次に、ステップS535において、読み出した記録再生器IDと所有するマスター鍵に基づいて暗号化コンテンツの復号に適用する鍵を生成する。この生成処理は、コンテンツ鍵 K_{con} を得るものである場合は、例えばコンテンツ鍵 $K_{con} = DES(MK_{con}, \text{記録再生器ID})$ となる。ステップS536で、この鍵を用いてコンテンツを復号する。

【0439】

この例においては、図54下段に示すように、記録再生器利用者と、システム管理者の双方がマスター鍵（例えばコンテンツ鍵生成用マスター鍵 MK_{con} ）を有し、コンテンツの暗号化、復号に必要な配送鍵を逐次的にそれぞれの所有するマスター鍵と各ID（記録再生器ID）に基づいて生成する。

【0440】

このシステムでは、万が一コンテンツ鍵が第三者に漏洩した場合、そのコンテンツの復号が第三者において可能となるが、記録再生器IDの異なる他の記録再生器用に暗号化されたコンテンツの復号は防止することが可能であるため、1つのコンテンツ鍵の漏洩がシステム全体に及ぼす影響を最小限にすることができるという効果がある。また、システム管理側、ユーザデバイス側両者において、コンテンツ毎の鍵の対応付けリストを保持する必要がないという効果もある。

【0441】

図55は、スレーブデバイス、例えばメモリカード等の記録デバイスと、ホストデバイス、例えば記録再生器間における相互認証処理に用いる認証鍵をマスター鍵に基づいて生成する構成である。先に説明した認証処理（図20参照）では、スレーブデバイスの内部メモリに認証鍵を予め格納した構成としてあるが、これを図55に示すように認証処理時にマスター鍵に基づいて生成する構成とすることができる。

【0442】

例えば記録デバイスであるスレーブデバイスは、認証処理開始前の初期化処理として、ステップS541において、記録デバイスであるスレーブデバイスの内部メモリに格納したマスター鍵とスレーブデバイスIDとに基づいて相互認証処

理に用いる認証鍵 K_{ake} を生成する。これは例えば、 $K_{ake} = DES(MK_{ake}, \text{スレーブデバイスID})$ によって生成する。次に、ステップ S542 において、生成した認証鍵をメモリに格納する。

【0443】

一方、例えば記録再生器等のホストデバイス側では、ステップ S543 において、装着された記録デバイス、すなわちスレーブデバイスから、通信手段を介してスレーブデバイスIDを読み出す。次に、ステップ S544 において、読み出したスレーブデバイスIDと所有する認証鍵生成用マスター鍵に基づいて相互認証処理に適用する認証鍵を生成する。この生成処理は、例えば認証鍵 $K_{ake} = DES(MK_{ake}, \text{スレーブデバイスID})$ となる。ステップ S545 で、この認証鍵を用いて認証処理を実行する。

【0444】

この例においては、図55下段に示すように、スレーブデバイスと、マスターデバイスの双方がマスター鍵、すなわち認証鍵生成用マスター鍵 MK_{ake} を有し、相互認証処理に必要な認証鍵を逐次的にそれぞれの所有するマスター鍵とスレーブデバイスIDに基づいて生成する。

【0445】

このシステムでは、万が一認証鍵が第三者に漏洩した場合、その認証鍵は、そのスレーブデバイスのみ有効であるため、他のスレーブデバイスとの関係においては、認証が成立しないことになり、鍵の漏洩によって発生する影響を最小限にすることができるという効果がある。

【0446】

このように、本発明のデータ処理装置においては、コンテンツプロバイダと記録再生器、あるいは記録再生器と記録デバイス間のような2つのエンティティ間における暗号情報処理に関する手続きに必要な鍵等の情報をマスター鍵と各IDから逐次的に生成する構成とした。従って、鍵情報が各エンティティから漏洩した場合でも、個別の鍵による被害の範囲はより限定され、また前述したような個別のエンティティごとの鍵リストの管理も不要となる。

【0447】

(13) 暗号処理における暗号強度の制御

上述した実施例において、記録再生器300と記録デバイス400間での暗号処理は、説明を理解しやすくするため、主として、先に図7を用いて説明したシングルDES構成による暗号処理を用いた例について説明してきた。しかしながら、本発明のデータ処理装置において適用される暗号化処理方式は上述したシングルDES方式に何ら限定されるものではなく、必要なセキュリティ状態に応じた暗号化方式を採用することが可能である。

【0448】

例えば先に説明した図8～図10の構成のようなトリプルDES方式を適用してもよい。例えば図3に示す記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の双方において、トリプルDES方式を実行可能な構成とし、図8～図10で説明したトリプルDES方式による暗号処理に対応する処理を実行する構成が可能である。

【0449】

しかしながら、コンテンツの提供者は、コンテンツに応じて処理速度を優先してコンテンツ鍵K_{con}をシングルDES方式による64ビット鍵構成とする場合もあり、また、セキュリティを優先してコンテンツ鍵K_{con}をトリプルDES方式による128ビット、または192ビット鍵構成とする場合もある。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の構成をトリプルDES方式、シングルDES方式いずれか一方の方式にのみ対応可能な構成とすることは好ましくない。従って、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401は、シングルDES、トリプルDESいずれの方式にも対応可能とする構成が望ましい。

【0450】

しかしながら、記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401の暗号処理構成をシングルDES方式、トリプルDES方式の双方を実行可能な構成とするためには、それぞれの別の回路、ロジックを構成しなければならない。例えば、記録デバイス400においてトリプルDESに対応する処理を実行するためには、先の図29に示すコマンドレジスタにトリプル

D E S の命令セットを新たに格納することが必要となる。これは記録デバイス 4 0 0 に構成する処理部の複雑化を招くこととなる。

【 0 4 5 1 】

そこで、本発明のデータ処理装置は、記録デバイス 4 0 0 側の暗号処理部 4 0 1 の有するロジックをシングル D E S 構成として、かつトリプル D E S 暗号化処理に対応した処理が実行可能で、トリプル D E S 方式による暗号化データ(鍵、コンテンツ等)を記録デバイスの外部メモリ 4 0 2 に格納することを可能とした構成を提案する。

【 0 4 5 2 】

例えば図 3 2 に示すデータフォーマットタイプ 0 の例において、記録再生器 3 0 0 から記録デバイス 4 0 0 に対してコンテンツデータのダウンロードを実行する際、先に説明したフォーマットタイプ 0 のダウンロードのフローを示す図 3 9 のステップ S 1 0 1 で認証処理を実行し、ここでセッション鍵 K s e s を生成する。さらに、ステップ S 1 1 7 において、記録再生器 3 0 0 側の暗号処理部 3 0 2 においてセッション鍵 K s e s によるコンテンツ鍵 K c o n の暗号化処理が実行され、この暗号化鍵が記録デバイス 4 0 0 に通信手段を介して転送され、ステップ S 1 1 8 において、この暗号化鍵を受信した記録デバイス 4 0 0 の暗号処理部 4 0 3 がセッション鍵 K s e s によるコンテンツ鍵 K c o n の復号処理を実行し、さらに、保存鍵 K s t r によるコンテンツ鍵 K c o n の暗号化処理を実行して、これを記録再生器 3 0 0 の暗号処理部 3 0 2 に送信し、その後、記録再生器 3 0 0 がデータフォーマットを形成(ステップ S 1 2 1)してフォーマット化されたデータを記録デバイス 4 0 0 に送信し、記録デバイス 4 0 0 が受信したデータを外部メモリ 4 0 2 に格納する処理を行なっている。

【 0 4 5 3 】

上記処理においてステップ S 1 1 7, S 1 1 8 間において実行される記録デバイス 4 0 0 の暗号処理部 4 0 1 での暗号処理をシングル D E S、またはトリプル D E S いずれかの方式を選択的に実行可能な構成とすれば、コンテンツ提供者がトリプル D E S にしたかったコンテンツ鍵 K c o n を用いたコンテンツデータを提供する場合も、またシングル D E S にしたかったコンテンツ鍵 K c o n を用

いたコンテンツデータを提供する場合も、いずれの場合にも対応可能となる。

【0454】

図56に本発明のデータ処理装置における記録再生器300の暗号処理部302と、記録デバイス400の暗号処理部401との双方を用いてトリプルDES方式に従った暗号処理方法を実行する構成を説明するフローを示す。図56では、一例として記録再生器300からコンテンツデータを記録デバイス400にダウンロードする際に実行される保存鍵Kstrを用いたコンテンツ鍵Kconの暗号化処理例であり、コンテンツ鍵KconがトリプルDES方式による鍵である場合の例を示している。なお、ここでは、コンテンツ鍵Kconを代表して、その処理例を示すが、他の鍵、またはコンテンツ等、その他のデータについても同様の処理が可能である。

【0455】

トリプルDES方式においては、先の図8～10において説明したように、シングルDESでは64ビット鍵、トリプルDES方式による場合は、128ビット、または192ビット鍵構成として、2つ、または3つの鍵が用いられる処理である。これら3つのコンテンツ鍵をそれぞれKcon1, Kcon2, (Kcon3)とする。Kcon3は用いられない場合もあるので、かっこで示している。

【0456】

図56の処理について説明する。ステップS301は記録再生器300と、記録デバイス400間での相互認証処理ステップである。この相互認証処理ステップは、先に説明した図20の処理によって実行される。なお、この認証処理の際、セッション鍵Ksesが生成される。

【0457】

ステップS301の認証処理が終了すると、ステップS302において、各チェック値、チェック値A、チェック値B、コンテンツチェック値、総チェック値、各ICVの照合処理が実行される。

【0458】

これらのチェック値(ICV)照合処理が終了し、データ改竄がないと判定さ

れると、ステップ S 3 0 3 に進み、記録再生器 3 0 0 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 を使って、先に取り出したまたは生成した配送鍵 K d i s を用いて、受信したメディア 5 0 0、または、通信部 3 0 5 を介して通信手段 6 0 0 から受信したデータのヘッダ部に格納されたコンテンツ鍵 K c o n の復号化処理を行う。この場合のコンテンツ鍵は、トリプル D E S 方式による鍵であり、コンテンツ鍵 K c o n 1, K c o n 2, (K c o n 3) である。

【 0 4 5 9 】

次に、ステップ S 3 0 4 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 において、ステップ S 3 0 3 で復号化したコンテンツ鍵 K c o n 1, K c o n 2, (K c o n 3) の中のコンテンツ鍵 K c o n 1 のみを相互認証の際に共有しておいたセッション鍵 K s e s で暗号化する。

【 0 4 6 0 】

記録再生器 3 0 0 の制御部 3 0 1 は、セッション鍵 K s e s で暗号化されたコンテンツ鍵 K c o n 1 を含むデータを記録再生器 3 0 0 の記録再生器暗号処理部 3 0 2 から読み出し、これらのデータを記録再生器 3 0 0 の記録デバイスコントローラ 3 0 3 を介して記録デバイス 4 0 0 に送信する。

【 0 4 6 1 】

次に、ステップ S 3 0 5 において、記録再生器 3 0 0 から送信されてきたコンテンツ鍵 K c o n 1 を受信した記録デバイス 4 0 0 は、受信したコンテンツ鍵 K c o n 1 を記録デバイス暗号処理部 4 0 1 の暗号／復号化部 4 0 6 に、相互認証の際に共有しておいたセッション鍵 K s e s で復号化する。さらに、ステップ S 3 0 6 において、記録デバイス暗号処理部 4 0 1 の内部メモリ 4 0 5 に保存してある記録デバイス固有の保存鍵 K s t r で再暗号化させて、通信部 4 0 4 を介して記録再生器 3 0 0 に送信する。

【 0 4 6 2 】

次に、ステップ S 3 0 7 において、記録再生器暗号処理部 3 0 2 の制御部 3 0 6 は、記録再生器暗号処理部 3 0 2 の暗号／復号化部 3 0 8 において、ステップ

S303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon2のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。

【0463】

記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたコンテンツ鍵Kcon2を含むデータを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

【0464】

次に、ステップS308において、記録再生器300から送信されてきたコンテンツ鍵Kcon2を受信した記録デバイス400は、受信したコンテンツ鍵Kcon2を記録デバイス暗号処理部401の暗号／復号化部406に、相互認証の際に共有しておいたセッション鍵Ksesで復号化する。さらに、ステップS309において、記録デバイス暗号処理部401の内部メモリ405に保存してある記録デバイス固有の保存鍵Kstrで再暗号化させて、通信部404を介して記録再生器300に送信する。

【0465】

次に、ステップS310において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308において、ステップS303で復号化したコンテンツ鍵Kcon1, Kcon2, (Kcon3)の中のコンテンツ鍵Kcon3のみを相互認証の際に共有しておいたセッション鍵Ksesで暗号化する。

【0466】

記録再生器300の制御部301は、セッション鍵Ksesで暗号化されたコンテンツ鍵Kcon3を含むデータを記録再生器300の記録再生器暗号処理部302から読み出し、これらのデータを記録再生器300の記録デバイスコントローラ303を介して記録デバイス400に送信する。

【0467】

次に、ステップS311において、記録再生器300から送信されてきたコン

テンツ鍵 K_{con3} を受信した記録デバイス 400 は、受信したコンテンツ鍵 K_{con3} を記録デバイス暗号処理部 401 の暗号／復号化部 406 に、相互認証の際に共有しておいたセッション鍵 K_{ses} で復号化する。さらに、ステップ S312 において、記録デバイス暗号処理部 401 の内部メモリ 405 に保存してある記録デバイス固有の保存鍵 K_{str} で再暗号化させて、通信部 404 を介して記録再生器 300 に送信する。

【0468】

次にステップ S313 において、記録再生器の暗号処理部は、図 32～35 で説明した各種のデータフォーマットを形成して、記録デバイス 400 に送信する。

【0469】

最後にステップ S314 において、記録デバイス 400 は、フォーマット形成が終了した受信データを外部メモリ 402 に格納する。このフォーマットデータには、保存鍵 K_{str} で暗号化されたコンテンツ鍵 K_{con1} , K_{con2} , (K_{con3}) を含んでいる。

【0470】

このような処理を実行することにより、記録デバイス 400 に格納するコンテンツ鍵をトリプル DES 方式の暗号方式による鍵として格納することが可能となる。なお、コンテンツ鍵が K_{con1} , K_{con2} の 2 つの鍵である場合は、ステップ S310～S312 の処理は省略される。

【0471】

このように、記録デバイス 400 は、同じ態様の処理、すなわちステップ S305, S306 の処理ステップを複数回、その対象を変更するのみで繰り返し実行することにより、トリプル DES の適用された鍵をメモリに格納可能となる。コンテンツ鍵 K_{con} がシングル DES の適用鍵である場合は、ステップ S305, S306 を実行して、ステップ S313 のフォーマット化処理を実行してメモリに格納すればよい。このような構成は、ステップ S305, S306 の処理を実行するコマンドを先に説明した図 29 のコマンドレジスタに格納し、この処理をコンテンツ鍵の態様、すなわちトリプル DES 方式か、シングル DES 方式

かによって、適宜 1 回～3 回実行する構成とすればよい。従って、記録デバイス 4 0 0 の処理ロジック中にトリプル D E S の処理方式を含ませることなく、トリプル D E S 方式、シングル D E S 方式、の双方の処理が可能となる。なお、暗号化方式については、コンテンツデータのヘッダ部内の取扱方針に記録し、これを参照することで判定することが可能である。

【 0 4 7 2 】

(1 4) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理

先に説明した図 4 ～ 6 のコンテンツデータ構成から理解されるように、本発明のデータ処理装置において利用されるコンテンツデータのヘッダ部に格納された取扱方針には、コンテンツタイプ、起動優先順位情報が含まれる。本発明のデータ処理装置における記録再生器 3 0 0 は、記録デバイス 4 0 0 、あるいは、D V D 、 C D 、ハードディスク、さらにはゲームカートリッジ等の各種記録媒体に記録されたアクセス可能なコンテンツデータが複数存在する場合、これらコンテンツの起動順位を起動優先順位情報に従って決定する。

【 0 4 7 3 】

記録再生器 3 0 0 は、各記録デバイス D V D 装置、C D ドライブ装置、ハードディスクドライブ装置等各種記録デバイスとの認証処理を実行後、コンテンツデータ中の優先順位情報に従って、最も優先順位の高いコンテンツデータ中のプログラムを優先して実行する。以下、この「コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」について説明する。

【 0 4 7 4 】

上述した本発明のデータ処理装置実施例の説明においては、記録再生器 3 0 0 が 1 つの記録デバイス 4 0 0 からコンテンツデータを再生、実行する場合の処理を中心として説明した。しかし、一般に記録再生器 3 0 0 は、図 2 に示すように記録デバイス 4 0 0 の他に、読み取り部 3 0 4 を介して D V D 、 C D 、ハードディスク、さらに、P I O 1 1 1 、 S I O 1 1 2 を介して接続されるメモリカード、ゲームカートリッジ等、各種記録媒体にアクセス可能な構成を有する。なお、図 2 では、図の複雑化を避けるため読み取り部 3 0 4 を 1 つのみ記載しているが

、記録再生器 3 0 0 は、異なる記憶媒体、例えば DVD、CD、フロッピーディスク、ハードディスクを並列に装着可能である。

【 0 4 7 5 】

記録再生器 3 0 0 は、複数の記憶媒体にアクセス可能であり、それぞれの記憶媒体にはそれぞれコンテンツデータが格納されている。例えば CD 等外部のコンテンツプロバイダが供給するコンテンツデータは、前述の図 4 のデータ構成でメディアに格納され、これらのメディアまたは、通信手段を介してダウンロードした場合には、図 2 6、図 2 7 のコンテンツデータ構成でメモリカード等の各記憶媒体に格納されている。さらに、具体的には、コンテンツデータのフォーマットタイプに応じて図 3 2 ～ 3 5 に示すようにメディア上、記録デバイス上でそれぞれ異なるフォーマットで格納される。しかし、いずれの場合にもコンテンツデータのヘッダ中の取扱方針にはコンテンツタイプ、起動優先順位情報が含まれる。

【 0 4 7 6 】

これら、複数のコンテンツデータに対するアクセスが可能な場合の記録再生器のコンテンツ起動処理をフローに従って説明する。

【 0 4 7 7 】

図 5 7 は、起動可能コンテンツが複数ある場合の処理例（1）を示す処理フローである。ステップ S 6 1 1 は、記録再生器 3 0 0 がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能な記録デバイスには、メモリカード、DVD 装置、CD ドライブ、ハードディスク装置、さらに、例えば P I O 1 1 1、S I O 1 1 2 を介して接続されるゲームカートリッジ等が含まれる。認証処理は、図 2 で示す制御部 3 0 1 の制御のもとに各記録デバイスに対して例えば先に図 2 0 で説明した手順に従って実行される。

【 0 4 7 8 】

次に、ステップ S 6 1 2 おいて、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

【 0 4 7 9 】

次に、ステップS613において、ステップS612で抽出された起動可能なプログラムにおける起動優先順位を判定する。これは、具体的には、ステップS612において選択された複数の起動可能なコンテンツデータのヘッダ中の取扱情報に含まれる優先情報を比較して最も高い優先順位を選択する処理である。

【0480】

次にステップS614で選択されたプログラムを起動する。なお、複数の起動可能なプログラムにおいて設定された優先順位が同じである場合には、記録デバイス間でデフォルトの優先順位を設定し、最優先されるデバイスに格納されたコンテンツプログラムを実行する。

【0481】

図58には、複数の記録デバイスに識別子を設定し、各識別子の付された記録デバイスについて順次、認証処理、コンテンツプログラム検索を実行する処理態様、すなわち起動可能コンテンツが複数ある場合の処理例(2)を示した。

【0482】

ステップS621では、記録再生器300に装着された記録デバイス(i)の認証処理(図20参照)を実行するステップである。複数(n個)の記録デバイスには順次1~nの識別子が付与されている。

【0483】

ステップS622では、ステップS621での認証が成功したか否かを判定し、認証が成功した場合は、ステップS623に進み、その記録デバイス(i)の記録媒体中から起動可能プログラムを検索する。認証が成功しなかった場合は、ステップS627に進み、新たなコンテンツ検索可能な記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS628に進み記録デバイス識別子iを更新し、ステップS621以降の認証処理ステップを繰り返す。

【0484】

ステップS623における処理は、記録デバイス(i)に格納されたコンテンツデータから起動可能なプログラムを検出する処理である。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムである

ものを抽出する処理として実行される。

【0485】

ステップS624では、コンテンツタイプがプログラムであるものが抽出されたか否かを判定し、抽出された場合は、ステップS625において、抽出プログラム中最も優先順位の高いものを選択し、ステップS626において選択プログラムを実行する。

【0486】

ステップS624において、コンテンツタイプがプログラムであるものが抽出されなかったと判定された場合には、ステップS627に進み、新たなコンテンツ検索記録デバイスの有無を判定し、無い場合は処理を終了し、記録デバイスが存在する場合は、ステップS628に進み記録デバイス識別子iを更新し、ステップS621以降の認証処理ステップを繰り返す。

【0487】

図59は、起動可能コンテンツが複数ある場合の処理例(3)を示す処理フローである。ステップS651は、記録再生器300がアクセス可能な記録デバイスの認証処理を実行するステップである。アクセス可能なDVD装置、CDドライブ、ハードディスク装置、メモリカード、ゲームカートリッジ等の認証処理を実行する。認証処理は、図2で示す制御部301の制御のもとに各記録デバイスに対して例えば先に図20で説明した手順に従って実行される。

【0488】

次に、ステップS652において、認証に成功した記録デバイス内のメモリに格納されたコンテンツデータから起動可能なプログラムを検出する。これは、具体的には、コンテンツデータの取扱方針に含まれるコンテンツタイプがプログラムであるものを抽出する処理として実行される。

【0489】

次に、ステップS653において、ステップS652で抽出された起動可能なプログラムの名称等の情報を表示手段に表示する。なお、表示手段は図2では示されていないが、AV出力データとして出力されたデータが図示しない表示手段に出力される構成となっている。なお、各コンテンツデータのプログラム名等の

ユーザ提供情報は、コンテンツデータの識別情報中に格納されており、図2に示すメインCPU106の制御のもとに制御部301を介して認証済みの各コンテンツデータのプログラム名称等、プログラム情報を出力手段に出力する。

【0490】

次にステップS654では、図2に示す入力インタフェース、コントローラ、マウス、キーボード等の入力手段からのユーザによるプログラム選択入力を入力インタフェース110を介してメインCPU106が受領し、選択入力にしたがって、ステップS655においてユーザ選択プログラムを実行する。

【0491】

このように本発明のデータ処理装置では、コンテンツデータ中のヘッダ内の取扱情報にプログラム起動優先順位情報を格納し、記録再生器300がこの優先順位に従ってプログラムを起動する、あるいは表示手段に起動プログラム情報を表示してユーザによって選択する構成としたので、ユーザがプログラムを検索する必要がなく、起動に要する時間およびユーザの労力を省くことが可能となる。また、起動可能なプログラムは、すべて記録デバイスの認証処理後に起動、または起動可能プログラムであることの表示がなされるので、プログラムを選択してから正当性の確認を行なう等の処理の煩雑性が解消される。

【0492】

(15) コンテンツ構成および再生(伸長)処理

本発明のデータ処理装置では、上述したように記録再生器300は、メディア500または通信手段600からコンテンツをダウンロード、あるいは記録デバイス400から再生処理を行う。上記の説明は、コンテンツのダウンロード、あるいは再生処理に伴う、暗号化データの処理を中心として説明してきた。

【0493】

図3の記録再生器300における制御部301は、コンテンツデータを提供するDVD等のデバイス500、通信手段600、記録デバイスからのコンテンツデータのダウンロード処理、または再生処理に伴う認証処理、暗号化、復号化処理全般を制御する。

【0494】

これらの処理結果として得られた再生可能なコンテンツは、例えば音声データ、画像データ等である。復号データは制御部 3 0 1 から図 2 に示すメイン CPU の制御下に置かれ、音声データ、画像データ等に応じて A V 出力部に出力される。しかし、コンテンツが例えば音声データであって M P 3 圧縮がなされていれば、図 2 に示す A V 出力部の M P 3 デコーダによって音声データの復号処理がなされて出力される。また、コンテンツデータが画像データであり、M P E G 2 圧縮画像であれば、A V 処理部の M P E G 2 デコーダによって伸長処理が実行されて出力されることになる。このように、コンテンツデータに含まれるデータは、圧縮（符号化）処理がなされている場合もあり、また圧縮処理の施されていないデータもあり、コンテンツに応じた処理を施して出力する。

【 0 4 9 5 】

しかしながら、圧縮処理、伸長処理プログラムには、様々な種類があり、コンテンツプロバイダから圧縮データを提供されても対応する伸長処理実行プログラムが無い場合は、これを再生することができないという事態が発生する。

【 0 4 9 6 】

そこで、本発明のデータ処理装置は、データコンテンツ中に、圧縮データとその復号（伸長）処理プログラムを併せて格納する構成、あるいは圧縮データと復号（伸長）処理プログラムとのリンク情報をコンテンツデータのヘッダ情報として格納する構成を開示する。

【 0 4 9 7 】

図 2 に示したデータ処理全体図から、本構成に関する要素および関連要素を簡潔にまとめた図を図 6 0 に示す。記録再生器 3 0 0 は、例えば D V D 、 C D 等のデバイス 5 0 0 、または通信手段 6 0 0 、あるいはコンテンツを格納したメモリカード等の記録デバイス 4 0 0 から様々なコンテンツの提供を受ける。これらのコンテンツは、音声データ、静止画像、動画像データ、プログラムデータ等であり、また暗号化処理の施されているもの、施されていないもの、また、圧縮処理がなされているもの、なされていないもの等、様々なデータが含まれる。

【 0 4 9 8 】

受領コンテンツが暗号化されている場合は、すでに上述した項目中で説明した

ような手法によって制御部301の制御、および暗号処理部302の暗号処理によって復号処理が実行される。復号されたデータはメインCPU106の制御下で、AV処理部に109に転送されて、AV処理部109のメモリ3090に格納された後、コンテンツ解析部3091においてコンテンツ構成の解析が実行される。例えばコンテンツ中にデータ伸長プログラムが格納されていれば、プログラム記憶部3093にプログラムを格納し、音声データ、画像データ等のデータが含まれていればこれらをデータ記憶部3092に記憶する。伸長処理部3094では、プログラム記憶部に記憶された例えばMP3等の伸長処理プログラムを用いてデータ記憶部3092に記憶された圧縮データの伸長処理を実行して、スピーカ3001、モニタ3002に出力される。

【0499】

次に、AV処理部109が制御部301を介して受領するデータの構成および処理のいくつかの例について説明する。なお、ここでは、コンテンツの例として音声データを示し、また圧縮プログラムの例としてMP3を適用したものを代表して説明するが、本構成は、音声データのみならず、画像データにも適用できるものであり、また、圧縮伸長処理プログラムについてもMP3のみならず、MP EG 2, 4等各種のプログラムを適用することが可能である。

【0500】

図61にコンテンツ構成例を示す。図61はMP3によって圧縮された音楽データ6102、MP3復号（伸長）処理プログラム6101を併せて1つのコンテンツとして構成した例である。これらのコンテンツは、1コンテンツとしてメディア500、あるいは記録デバイス400に格納され、または通信手段600から配信される。記録再生器300は、これらのコンテンツが先に説明した通り、暗号化されているものであれば、暗号処理部303によって復号処理を実行した後、AV処理部109に転送される。

【0501】

AV処理部109のコンテンツ解析部3091では、受け取ったコンテンツを解析し、音声データ伸長プログラム（MP3デコーダ）部と、圧縮音声データ部からなるコンテンツから、音声データ伸長プログラム（MP3デコーダ）部を取

り出してプログラム記憶部 3 0 9 3 にプログラムを記憶し、圧縮音声データをデータ記憶部 3 0 9 2 に記憶する。なお、コンテンツ解析部 3 0 9 1 は、コンテンツとは別に受領したコンテンツ名、コンテンツ構成情報等の情報を受領したり、あるいはコンテンツ内に含まれるデータ名等の識別データ、データ長、データ構成等を示すデータに基づいてコンテンツ解析を実行してもよい。次に、圧縮伸長処理部 3 0 9 4 は、プログラム記憶部 3 0 9 3 に記憶された音声データ伸長プログラム（MP 3 デコーダ）に従ってデータ記憶部 3 0 9 2 に記憶された MP 3 圧縮音声データの伸長処理を実行して、AV 処理部 1 0 9 は伸長した音声データをスピーカ 3 0 0 1 に出力する。

【0502】

図 6 2 に図 6 1 のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップ S 6 7 1 は、AV 処理部 1 0 9 のメモリ 3 0 9 0 に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のデータから取り出し、モニタ 3 0 0 2 に表示する。ステップ S 6 7 2 は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース 1 1 0 を介して受領し、CPU 1 0 6 の制御のもとにユーザ入力データに基づく再生処理命令を AV 処理部 1 0 9 に出力する。AV 処理部 1 0 9 は、ステップ S 6 7 3 においてユーザ選択によるデータの抽出、伸長処理を実行する。

【0503】

次に図 6 3 に、1 つのコンテンツには圧縮音声データ、あるいは伸長処理プログラムのいずれか一方が含まれ、さらに各コンテンツのヘッダ情報としてコンテンツの内容を示すコンテンツ情報が含まれる構成例を示す。

【0504】

図 6 3 に示すように、コンテンツがプログラム 6 2 0 2 である場合は、ヘッダ情報 6 2 0 1 としてプログラムであること、およびプログラム種類が MP 3 伸長プログラムであることを示すコンテンツ識別情報が含まれる。一方、音声データ 6 2 0 4 をコンテンツとして含む場合は、ヘッダ 6 2 0 3 のコンテンツ情報には MP 3 圧縮データであるとの情報が含まれる。このヘッダ情報は、前述した例え

ば図4に示すコンテンツデータ構成の取扱方針（図5参照）中に含まれるデータから再生に必要な情報のみを選択してAV処理部109へ転送するコンテンツに付加して構成することが可能である。具体的には、図5に示す「取扱方針」中の各構成データに暗号処理部302において必要となる取扱方針データと、AV処理部109における再生処理時に必要となるデータとの識別値を付加し、これら識別値が、AV処理部109において必要であることを示すもののみを抽出してヘッダ情報とすることができる。

【0505】

図63に示す各コンテンツを受領したAV処理部109のコンテンツ解析部3091は、ヘッダ情報に従って、プログラムである場合はプログラムコンテンツをプログラム記憶部3093に記憶し、データである場合は、データコンテンツをデータ記憶部3092に記憶する。その後、圧縮伸長処理部3094は、データ記憶部からデータを取り出して、プログラム記憶部3093に記憶したMP3プログラムに従って伸長処理を実行して出力する。なお、プログラム記憶部3093にすでに同一プログラムが格納されている場合は、プログラム格納処理は省略してもよい。

【0506】

図64に図63のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS675は、AV処理部109のメモリ3090に格納されたデータ名、例えば音楽データのコンテンツであれば曲名等の情報をコンテンツとは別に受領した情報、あるいはコンテンツ内のヘッダから取り出し、モニタ3002に表示する。ステップS676は、ユーザの選択をスイッチ、キーボード等の各種入力手段から入力インタフェース110を介して受領する。

【0507】

次に、ステップS677では、ユーザ選択に対応するデータの再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、記録再生機器300のアクセス可能な範囲を最大検索範囲とすることが好ましく、例えば図60に示す、各メディア500、通信手段600、記録デバイス400等も検索範囲とする。

【0508】

AV処理部109に渡されるコンテンツはデータ部のみであり、プログラムコンテンツは記録再生器300内の他の記録媒体に格納される場合もあり、DVD、CD等のメディアを介してコンテンツ提供者から提供されることもある。従って、検索対象を記録再生機器300のアクセス格納範囲を検索範囲とする。検索の結果として再生プログラムが見つかり、CPU106の制御のもとにユーザ入力データに基づく再生処理命令をAV処理部109に出力する。AV処理部109は、ステップS679においてユーザ選択によるデータの抽出、伸長処理を実行する。また、別の実施例として、プログラムの検索をステップS675より前に行い、ステップS675においては、プログラムが検出されたデータのみを表示するようにしてもよい。

【0509】

次に図65に、1つのコンテンツに圧縮音声データ6303、伸長処理プログラム6302が含まれ、さらにコンテンツのヘッダ情報6301としてコンテンツの再生優先順位情報が含まれる構成例を示す。これは、先の図61のコンテンツ構成にヘッダ情報として再生優先順位情報を付加した例である。これは、前述の「(14) コンテンツデータにおける取扱方針中の起動優先順位に基づくプログラム起動処理」と同様、AV処理部109が受領したコンテンツ間において設定された再生優先順位に基づいて再生順を決定するものである。

【0510】

図66に図65のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS681は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS682において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択し、ステップS683において、選択されたデータの再生処理を実行する。

【0511】

次に図67に、1つのコンテンツにヘッダ情報とプログラムデータ6402、

あるいはヘッダ情報6403と、圧縮データ6404のいずれかの組合せから成る例において、データコンテンツのヘッダ6403にのみ、再生優先順位情報が付加されている構成例を示す。

【0512】

図68に図67のコンテンツ構成を持つデータの再生処理の一例を示すフローを示す。ステップS691は、AV処理部109のメモリ3090に格納されたデータ、すなわち再生対象データのデータ情報を検索リストに設定する。検索リストはAV処理部109内のメモリの一部領域を使用して設定する。次に、ステップS692において、AV処理部109のコンテンツ解析部3091において検索リストから優先順位の高いデータを選択する。

【0513】

次に、ステップS693では、選択されたデータに対応するデータ再生用プログラム（例えばMP3）を検索する。このプログラム検索対象は、先の図64のフローにおける処理と同様、記録再生機器300のアクセス格納範囲を最大検索範囲とすることが好ましく、例えば図60に示す各メディア500、通信手段600、記録デバイス400等も検索範囲とする。

【0514】

検索の結果として再生プログラムが見つかる（ステップS694でYes）と、ステップS695において、選択されたデータを検索の結果得られたプログラムを用いて、伸長再生処理を実行する。

【0515】

一方、検索結果としてプログラムが検出されなかった場合（ステップS694でYes）は、ステップS696に進み、ステップS691で設定した検索リスト中に含まれる他のデータにおいて、同一のプログラムを用いた再生処理が必要なものを削除する。これは、新たにそのデータに対する再生プログラム検索を実行しても検出されないことが明らかであるからである。さらに、ステップS697において検索リストが空であるかを判定し、からでない場合は、ステップS692に戻り、さらに次の優先順位の高いデータを抽出して、プログラム検索処理を実行する。

【0516】

このように、本構成によれば、圧縮処理されたコンテンツは、その復号(伸長)プログラムと共に構成されるか、あるいはコンテンツが圧縮されたデータのみ、あるいは伸長処理プログラムのみである場合は、それぞれのコンテンツにコンテンツがどのような圧縮データであるのか、あるいはどのような処理を実行するかを示すヘッダ情報を有しているので、コンテンツを受領した処理部(例えばAV処理部)は、圧縮データに付属する伸長処理プログラムを用いて伸長再生処理を実行するか、あるいは伸長処理プログラムを圧縮データのヘッダ情報に基づいて検索して、検索の結果得られたプログラムにしたがって伸長再生処理を実行するので、ユーザによるデータの伸長プログラムの選択、検索等の処理が不要となりユーザ負担が軽減され、効率的なデータ再生が可能となる。さらに、ヘッダに再生優先順位情報を有した構成によれば、再生順序を自動設定する構成が可能となり、ユーザによる再生順設定の操作を省略することができる。

【0517】

なお、上述の実施例では、圧縮音声データコンテンツ、および音声圧縮データの伸長処理プログラムとしてのMP3を例として説明したが、圧縮データを含むコンテンツ、圧縮画像データの伸長処理プログラムを有するコンテンツであっても本構成は同様に適用可能であり、同様の効果を奏するものである。

【0518】

(16) セーブデータの生成および記録デバイスへの格納、再生処理

本発明のデータ処理装置は、例えば記録再生器300において実行されるコンテンツがゲームプログラム等である場合等、ゲームプログラムを途中で中断して、所定時間後、新たに再開したい場合には、その中断時点のゲーム状態等をセーブ、すなわち記録デバイスに格納し、これを再開時に読み出してゲームを続行することが可能な構成を持つ。

【0519】

従来のゲーム機器、パソコン等の記録再生器におけるセーブデータ保存構成は、例えば記録再生器に内蔵、あるいは外付け可能なメモリカード、フロッピーディスク、ゲームカートリッジ、あるいはハードディスク等の記憶媒体にセーブデ

ータを保存する構成を持つが、特に、そのセーブデータに対するセキュリティ確保構成を有しておらず、例えばゲームアプリケーションプログラムに共通の仕様でデータのセーブ処理が行われる構成となっている。

【0520】

従って、例えばある1つの記録再生器Aを用いてセーブされたセーブデータが別のゲームプログラムによって使用されたり、書換えられたりする事態が発生し、従来、セーブデータのセキュリティはほとんど考慮されていなかったのが実状である。

【0521】

本発明のデータ処理装置は、このようなセーブデータのセキュリティ確保を実現可能とした構成を提供する。例えばあるゲームプログラムのセーブデータは、そのゲームプログラムのみが使用可能な情報に基づいて暗号化して記録デバイスに格納する。あるいは、記録再生器固有の情報に基づいて暗号化して記録デバイスに格納する。これらの手法により、セーブデータの利用を特定の機器、特定のプログラムだけに制限することができ、セーブデータのセキュリティが確保される。以下、本発明のデータ処理装置における「セーブデータの生成および記録デバイスへの格納、再生処理」について説明する。

【0522】

図69に本発明のデータ処理装置におけるセーブデータ格納処理について説明するブロック図を示す。DVD、CD等のメディア500、あるいは通信手段600からコンテンツが記録再生器300に提供される。提供されるコンテンツは、先に説明したようにコンテンツ固有の鍵であるコンテンツ鍵K_{con}によって暗号化されており、記録再生器300は、前述した「(7)記録再生器から記録デバイスへのダウンロード処理」の欄で説明(図22参照)した処理に従ってコンテンツ鍵を取得して、暗号化コンテンツを復号した後、記録デバイス400に格納する。ここでは、記録再生器300がコンテンツプログラムをメディア、通信手段から復号して再生、実行を行ない、実行の後、得られるセーブデータを外付け、あるいは内蔵のメモ리카ード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納し、再生する処理、あるいはコン

テンツを記録デバイス400Aにダウンロードした後、記録デバイス400Aからコンテンツを再生、実行して、そのセーブデータを外付け、あるいは内蔵のメモリカード、ハードディスク等の各種の記録デバイス400A、400B、400Cのいずれかに格納する処理記録デバイス400に格納し、再生する処理について説明する。

【0523】

記録再生器300には、先に説明したように記録再生器識別子IDdev、システムに共通な署名鍵であるシステム署名鍵Ksys、個々の記録再生器に固有の署名鍵である記録再生器署名鍵Kdev、さらに各種の個別鍵を生成するマスタ鍵を有する。マスタ鍵については、「(12)マスタ鍵に基づく暗号処理鍵生成構成」において、詳しく説明した通り、例えば、配送鍵Kdis、あるいは認証鍵Kake等を生成する鍵である。ここでは、特にマスタ鍵の種類を限定することなく記録再生器300の有するマスタ鍵全般を代表するものとしてMKxとして示す。図69の下段には、セーブデータの暗号鍵Ksavの例を示した。セーブデータ暗号鍵Ksavは、セーブデータを各種記録デバイス400A～Cに格納する場合の暗号化処理、そして、各種記録デバイス400A～Cから再生する際の復号処理に用いられる暗号鍵である。図70以下を用いて、セーブデータの格納処理および再生処理の例を説明する。

【0524】

図70は、コンテンツ個有鍵、システム共通鍵のいずれかを用いてセーブデータを記録デバイス400A～Cいずれかに格納する処理のフロー図である。なお、各フローにおける処理は記録再生器300が実行する処理であり、各フローでセーブデータを格納する記録デバイスは内蔵、外付け記録デバイス400A～Cのいずれかであればよく、いずれかに限定さるものではない。

【0525】

ステップS701は、コンテンツ識別子、例えばゲームIDを記録再生器300が読み出す処理である。これは、先に説明した図4、26、27、32～35に示すコンテンツデータ中の識別情報に含まれるデータであり、セーブデータの格納処理命令を図2に示す入力インタフェース110を介して受領したメインC

P U 1 0 6 がコンテンツ識別子の読み取りを制御部 3 0 1 に指示する。

【0526】

制御部 3 0 1 は、実行プログラムが DVD、CD-ROM 等、読取部 3 0 4 を介して実行されているコンテンツの場合は、読取部 3 0 4 を介してコンテンツデータ中のヘッダに含まれる識別情報を取り出し、実行プログラムが、記録デバイス 4 0 0 に格納されたコンテンツである場合は、記録デバイスコントローラ 3 0 3 を介して識別情報を取り出す。なお、記録再生器 3 0 0 がコンテンツプログラムを実行中で、すでに記録再生器中の RAM、その他のアクセス可能な記録媒体にコンテンツ識別子が格納済みである場合は、新たな読み取り処理を実行せずに、読み込み済みデータに含まれる識別情報を利用してもよい。

【0527】

次に、ステップ S 7 0 2 は、プログラムの使用制限を行なうか否かによって処理を変更するステップである。プログラム使用制限とは、保存するセーブデータをそのプログラムのみに固有に利用可能とする制限を付するか否かを設定する制限情報であり、プログラムのみに固有に利用可能とする場合は、「プログラム使用制限あり」とし、プログラムに利用を拘束されないセーブデータとする場合を「プログラム使用制限なし」とする。これは、ユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよく、設定された制限情報は、図 6 9 の記録デバイス 4 0 0 A ~ C にデータ管理ファイルとして格納される。

【0528】

データ管理ファイルの例を図 7 1 に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図 6 9 に示す [I D d e v] である。プログラム使用制限は、上述したように保存するセーブデータをそのプログラムのみに固有に利用可能とす場合、「する」の設定とし、対応プログラムに制限されない利用を可能とする場合「しない」の設定となる。プログラム使用制限

は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

【0529】

図70に戻り、フローの説明を続ける。ステップS702において、プログラム使用制限について「する」の設定がされている場合は、ステップS703に進む。ステップS703では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Kconを読み出してコンテンツ固有鍵をセーブデータ暗号鍵Ksavとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ暗号鍵Ksavを生成する。

【0530】

一方、ステップS702において、プログラム使用制限について「しない」の設定がされている場合は、ステップS707に進む。ステップS707では、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ksysを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ksysをセーブデータ暗号鍵Ksavとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0531】

次に、ステップS704において、ステップS703、またはステップS707で選択、または生成されたセーブデータ暗号化鍵Ksavを用いてセーブデータの暗号化処理を実行する。この暗号化処理は、図2における暗号処理部302が例えば前述のDESアルゴリズムを適用して実行する。

【0532】

ステップS704において暗号化処理されたセーブデータは、ステップS705において記録デバイスに格納される。セーブデータを格納可能な記録デバイスが図69に示すように複数ある場合は、ユーザが記録デバイス400A～Cのいずれかをセーブデータ格納先として予め選択する。さらに、ステップS706に

において先に図 7 1 を用いて説明したデータ管理ファイルに先にステップ S 7 0 2 で設定したプログラム使用制限情報の書き込み、すなわちプログラム使用制限「する」または「しない」の書き込みを実行する。

【 0 5 3 3 】

以上で、セーブデータの格納処理が終了する。ステップ S 7 0 2 において Yes、すなわち「プログラム使用制限する」の選択がなされ、ステップ S 7 0 3 においてコンテンツ固有鍵に基づいて生成されたセーブデータ暗号化鍵 K s a v によって暗号化処理されたセーブデータは、コンテンツ固有鍵情報を持たないコンテンツプログラムによる復号処理が不可能となり、セーブデータは同じコンテンツ鍵情報を有するコンテンツプログラムのみが利用できることになる。ただし、ここでは、セーブデータ暗号化鍵 K s a v は記録再生器固有の情報に基いて生成されたものではないので、例えばメモリカード等の着脱可能な記録デバイスに格納されたセーブデータは異なる記録再生器においても対応するコンテンツプログラムと共に使用する限り再生可能となる。

【 0 5 3 4 】

また、ステップ S 7 0 2 において No、すなわち「プログラム使用制限しない」の選択がなされ、ステップ S 7 0 7 においてシステム共通鍵に基づくセーブデータ暗号化鍵 K s a v によって暗号化処理されたセーブデータは、コンテンツ識別子が異なるプログラムを用いた場合でも、また、記録再生器が異なっていた場合でも再生して利用することが可能となる。

【 0 5 3 5 】

図 7 2 は、図 7 0 のセーブデータ格納処理によって格納されたセーブデータを再生する処理を示したフローである。

【 0 5 3 6 】

ステップ S 7 1 1 は、コンテンツ識別子、例えばゲーム I D を記録再生器 3 0 0 が読み出す処理である。これは、先に説明した図 7 0 のセーブデータ格納処理のステップ S 7 0 1 と同様の処理であり、コンテンツデータ中の識別情報に含まれるデータを読み出す処理である。

【 0 5 3 7 】

次に、ステップS712では、図69に示す記録デバイス400A～Cから、図71を用いて説明したデータ管理ファイルを読み出し、ステップS711において読み出したコンテンツ識別子、および対応して設定された使用プログラム制限情報を抽出する。データ管理ファイルに設定されたプログラム使用制限が「する」であった場合は、ステップS714に進み、「しない」であった場合には、ステップS717に進む。

【0538】

ステップS714では、コンテンツデータからコンテンツ固有の鍵、例えば先に説明したコンテンツ鍵Kconを読み出してコンテンツ固有鍵をセーブデータ復号化鍵Ksavとするか、あるいはコンテンツ固有鍵に基づいてセーブデータ復号化鍵Ksavを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【0539】

一方、ステップS712において、データ管理ファイルの設定がプログラム使用制限について「しない」の設定であった場合は、ステップS717において、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ksysを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ksysをセーブデータ復号化鍵Ksavとするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0540】

次に、ステップS715において、ステップS714、またはステップS717で選択、または生成されたセーブデータ復号化鍵Ksavを用いてセーブデータの復号化処理を実行し、ステップS716において、復号したセーブデータを記録再生器300において再生、実行する。

【0541】

以上で、セーブデータの再生処理が終了する。上述のようにデータ管理ファイルに「プログラム使用制限する」の設定がなされている場合は、コンテンツ固有鍵に基づいてセーブデータ復号化鍵が生成され、「プログラム使用制限しない」の設定がある場合はシステム共通鍵に基づいてセーブデータ復号化鍵が生成される。「プログラム使用制限する」の設定がされている場合、使用しているコンテンツのコンテンツ識別子が同じものでないとセーブデータの復号処理の可能な復号化鍵を得ることができないこととなり、セーブデータのセキュリティを高めることが可能となる。

【0542】

図73、図74は、コンテンツ識別子を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図73）、セーブデータ再生処理フロー（図74）である。

【0543】

図73において、ステップS721～S722は、図70のステップS701～S702と同様の処理であり、説明を省略する。

【0544】

図73のセーブデータ格納処理フローは、ステップS722において「プログラム使用制限する」の設定を行なった場合、ステップS723においてコンテンツデータからコンテンツ識別子、すなわちコンテンツIDを読み出してコンテンツIDをセーブデータ暗号化鍵Ksavとするか、あるいはコンテンツIDに基づいてセーブデータ暗号化鍵Ksavを生成する。例えば、記録再生器300の暗号処理部307はコンテンツデータから読み出したコンテンツIDに、記録再生器300の内部メモリに格納されたマスター鍵MKxを適用して、例えばDES（MKx，コンテンツID）によってセーブデータ暗号化鍵Ksavを得ることができる。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0545】

一方、ステップS722において、プログラム使用制限について「しない」の

設定とした場合は、ステップS727において、記録再生器300内に格納されたシステム共通鍵、例えばシステム署名鍵Ksysを記録再生器300の内部メモリ307から読み出して、システム署名鍵Ksysをセーブデータ暗号化鍵Ksavとするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0546】

ステップS724以下の処理は、前述の図70の処理フローにおけるステップS704以下の処理と同様であり、説明を省略する。

【0547】

さらに、図74は、図73のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップS731～S733は前述の図72の対応処理と同様であり、ステップS734のみが異なる。ステップS734においては、コンテンツデータからコンテンツ識別子、すなわちコンテンツIDを読み出してコンテンツIDをセーブデータ復号化鍵Ksavとするか、あるいはコンテンツIDに基づいてセーブデータ復号化鍵Ksavを生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるコンテンツ識別子に基づいて暗号化されたデータは、同一のコンテンツ識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【0548】

以下の処理、ステップS735、S736、S737は、図72の対応処理と同様であるので説明を省略する。図73、図74のセーブデータ格納および再生処理に従えば、プログラム使用制限するの設定を行なった場合、コンテンツIDを使用してセーブデータ暗号化鍵、復号化鍵を生成する構成としたので、先のコンテンツ固有鍵を使用したセーブデータ格納、再生処理と同様、対応するコンテンツプログラムが整合する場合以外は、セーブデータを利用することができない構成となり、セーブデータセキュリティを高めた保存が可能となる。

【0549】

図75、図77は、記録再生器固有鍵を用いてセーブデータの暗号化鍵、復号化鍵を生成するセーブデータ格納処理フロー（図75）、セーブデータ再生処理フロー（図77）である。

【0550】

図75において、ステップS741は、図70のステップS701と同様の処理であり、説明を省略する。ステップS742は、記録再生器の制限をするかしないかを設定するステップである。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。ステップS742において「記録再生器制限する」の設定をすると、ステップS743に進み、「しない」の設定をするとステップS747に進む。

【0551】

データ管理ファイルの例を図76に示す。データ管理ファイルは項目としてデータ番号、コンテンツ識別子、記録再生器識別子、記録再生器制限を含むテーブルとして生成される。コンテンツ識別子は、セーブデータを格納する対象となったコンテンツプログラムの識別データである。記録再生器識別子は、セーブデータを格納した記録再生器の識別子、例えば図69に示す[*IDdev*]である。記録再生器制限は、セーブデータを利用可能な記録再生器を限定する場合、すなわちセーブデータを生成し格納した記録再生器にのみ利用可能とする場合を「する」と設定し、他の記録再生器でも利用可能とする場合を「しない」の設定とするものである。記録再生器制限情報は、コンテンツプログラムを利用するユーザが任意に設定できるようにしてもよいし、コンテンツ製作者が設定して、この情報をコンテンツプログラム中に格納しておいてもよい。

【0552】

図75のセーブデータ格納処理フローにおいては、ステップS742において「記録再生器制限する」の設定を行なった場合、ステップS743において記録再生器300から記録再生器固有鍵、例えば記録再生器署名鍵*Kdev*を記録再

生器 3 0 0 の内部メモリ 3 0 7 から読み出して記録再生器署名鍵 K_{dev} をセーブデータ暗号化鍵 K_{sav} とするか、あるいは記録再生器署名鍵 K_{dev} に基づいてセーブデータ暗号化鍵 K_{sav} を生成する。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

【0553】

一方、ステップ S 7 4 2 において、記録再生器制限について「しない」の設定とした場合は、ステップ S 7 4 7 において、記録再生器 3 0 0 内に格納されたシステム共通鍵、例えばシステム署名鍵 K_{sys} を記録再生器 3 0 0 の内部メモリ 3 0 7 から読み出して、システム署名鍵 K_{sys} をセーブデータ暗号化鍵 K_{sav} とするか、あるいはシステム署名鍵に基づいてセーブデータ暗号化鍵 K_{sav} を生成する。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

【0554】

ステップ S 7 4 4、S 7 4 5 の処理は、前述の図 7 0 の処理フローにおける対応処理と同様であり、説明を省略する。

【0555】

ステップ S 7 4 6 では、データ管理ファイル（図 7 6 参照）にコンテンツ識別子、記録再生器識別子、そしてステップ 7 4 2 でユーザが設定した記録再生器制限情報「する／しない」を書き込む。

【0556】

さらに、図 7 7 は、図 7 5 のセーブデータ格納処理フローで記録デバイスに格納されたセーブデータを再生、実行する処理フローであり、ステップ S 7 5 1 は前述の図 7 2 の対応処理と同様、コンテンツ識別子を読み出す。次に、ステップ S 7 5 2 においては、記録再生器 3 0 0 内のメモリに格納された記録再生器識別子 (ID_{dev}) を読み出す。

【0557】

ステップ S 7 5 3 では、データ管理ファイル（図 7 6 参照）からコンテンツ識

別子、記録再生器識別子、設定済みの記録再生器制限情報「する／しない」の各情報を読み出す。データ管理ファイル中のコンテンツ識別子が一致するエントリにおいて、記録再生器制限情報が「する」に設定されている場合、テーブルエントリの記録再生器識別子がステップ S 7 5 2 で読み取られた記録再生器識別子と異なる場合は処理を終了する。

【 0 5 5 8 】

次に、ステップ S 7 5 4 でデータ管理ファイルの設定が「記録再生器制限する」である場合は、ステップ S 7 5 5 に進み、「しない」である場合は、ステップ S 7 5 8 に進む。

【 0 5 5 9 】

ステップ S 7 5 5 においては、記録再生器 3 0 0 から記録再生器固有鍵、例えば記録再生器署名鍵 K_{dev} を記録再生器 3 0 0 の内部メモリ 3 0 7 から読み出して記録再生器署名鍵 K_{dev} をセーブデータ復号化鍵 K_{sav} とするか、あるいは記録再生器署名鍵 K_{dev} に基づいてセーブデータ復号化鍵 K_{sav} を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器固有鍵に基づいて暗号化されたデータは、同一の記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

【 0 5 6 0 】

一方ステップ S 7 5 8 においては、記録再生器 3 0 0 内に格納されたシステム共通鍵、例えばシステム署名鍵 K_{sys} を記録再生器 3 0 0 の内部メモリ 3 0 7 から読み出して、システム署名鍵 K_{sys} をセーブデータ復号化鍵 K_{sav} とするか、あるいはシステム署名鍵に基づいてセーブデータ復号化鍵 K_{sav} を生成する。または、別途、記録再生器 3 0 0 の内部メモリ 3 0 7 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。以下のステップ S 7 5 6, S 7 5 7 は、前述のセーブデータ再生処理フローの対応ステップと同様の処理である。

【0561】

図75、図77に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器固有鍵によって暗号化、復号化処理が実行されるため、同一の記録再生器固有鍵を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

【0562】

次に、図78、図79に記録再生器識別子を用いてセーブデータの暗号化、復号化鍵を生成して格納、再生する処理フローを示す。

【0563】

図78は、記録再生器識別子を用いてセーブデータの暗号化を行い記録デバイスに格納する。ステップS761～S763は、先の図75と同様の処理である。ステップS764では、記録再生器から読み出した記録再生器識別子（IDdev）を用いてセーブデータの暗号化鍵Ksavを生成する。IDdevをセーブデータ暗号化鍵Ksavとして適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵MKxを適用して、DES（MKx，IDdev）によってセーブデータ暗号化鍵Ksavを得る等、IDdevに基づいてセーブデータ暗号化鍵ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0564】

以下の処理ステップS765～S768は、前述の図75の対応処理と同様であり、説明を省略する。

【0565】

図79は、図78の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS771～S774は、前述の図77の対応処理と同様である。

【0566】

ステップS775では、記録再生器から読み出した記録再生器識別子（IDdev）を用いてセーブデータの復号化鍵Ksavを生成する。IDdevをセー

ブデータ復号化鍵 K_{sav} として適用するか、あるいは記録再生器300の内部メモリに格納されたマスター鍵 MK_x を適用して、 $DES(MK_x, ID_{dev})$ によってセーブデータ復号化鍵 K_{sav} を得る等、 ID_{dev} に基づいてセーブデータ復号化鍵 K_{sav} を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、ある記録再生器識別子に基づいて暗号化されたデータは、同一の記録再生器識別子に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵 K_{sav} として使用してもよい。

【0567】

以下の処理ステップS776～S778は前述の図76の対応ステップの処理と同様である。

【0568】

この図78、図79に示すセーブデータ格納、再生処理フローによれば、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが可能となる。

【0569】

次に図80～82を用いて、上述のプログラム使用制限、および記録再生器使用制限を併せて実行するセーブデータ格納、再生処理について説明する。

【0570】

図80は、セーブデータ格納処理フローである。ステップS781において、コンテンツ識別子をコンテンツデータから読み出し、ステップS782において、プログラム使用制限判定を行ない、ステップS783において記録再生器制限判定を行なう。

【0571】

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップS785において、コンテンツ固有鍵(ex. K_{con})と、記録再生器固有

鍵 (K_{dev}) の双方に基づいてセーブデータ暗号化鍵 K_{sav} が生成される。これは、例えば $K_{sav} = (K_{con} \text{ XOR } K_{dev})$ 、あるいは記録再生器 300 の内部メモリに格納されたマスタ鍵 MK_x を適用して $K_{sav} = DES(MK_x, K_{con} \text{ XOR } K_{dev})$ 等によって得ることができる。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 K_{sav} として使用してもよい。

【0572】

「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップ S786 において、コンテンツ固有鍵 (ex. K_{con}) をセーブデータ暗号化鍵 K_{sav} とするか、あるいはコンテンツ固有鍵 (ex. K_{con}) に基づいてセーブデータ暗号化鍵 K_{sav} を生成する。

【0573】

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップ S787 において、記録再生器固有鍵 (K_{dev}) をセーブデータ暗号化鍵 K_{sav} とするか、あるいは記録再生器固有鍵 (K_{dev}) に基づいてセーブデータ暗号化鍵 K_{sav} が生成される。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 K_{sav} として使用してもよい。

【0574】

さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップ S787 において、システム共通鍵、例えばシステム署名鍵 K_{sys} をセーブデータ暗号化鍵 K_{sav} とするか、あるいはシステム署名鍵 K_{sys} に基づいてセーブデータ暗号化鍵 K_{sav} を生成する。または、別途、記録再生器 300 の内部メモリ 307 内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号化鍵 K_{sav} として使用してもよい。

【0575】

ステップ S789 では、ステップ S785～S788 のいずれかで生成されたセーブデータ暗号化鍵 K_{sav} によってセーブデータが暗号化され、記録デバイスに格納される。

【0576】

さらに、ステップS790では、ステップS782、S783において設定した制限情報がデータ管理ファイルに格納される。データ管理ファイルは、例えば図81に示す構成となり、項目としてデータ番号、コンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限を含む。

【0577】

図82は、図80の処理によって記録デバイスに格納されたセーブデータを再生、実行する処理フローである。ステップS791では、実行プログラムのコンテンツ識別子、記録再生器識別子を読み出し、ステップS792において、図81に示すデータ管理ファイルからコンテンツ識別子、記録再生器識別子、プログラム使用制限、記録再生器制限情報を読み出す。この場合、プログラム使用制限が「する」でコンテンツ識別子が不一致である場合、または記録再生器制限情報が「する」で記録再生器識別子が不一致である場合は、処理を終了する。

【0578】

次に、ステップS793、S794、S795では、データ管理ファイルの記録データにしたがって復号鍵生成処理をステップS796～S799の4態様のいずれかに設定する。

【0579】

「プログラム使用制限あり」、かつ「記録再生器制限あり」の場合は、ステップS796において、コンテンツ固有鍵(ex. Kcon)と、記録再生器固有鍵(Kdev)の双方に基づいてセーブデータ復号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。「プログラム使用制限あり」、かつ「記録再生器制限なし」の場合は、ステップS797において、コンテンツ固有鍵(ex. Kcon)をセーブデータ復号化鍵Ksavとするか、あるいはコンテンツ固有鍵(ex. Kcon)に基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0580】

「プログラム使用制限なし」、かつ「記録再生器制限あり」の場合は、ステップS798において、記録再生器固有鍵(Kdev)をセーブデータ復号化鍵Ksavとするか、あるいは記録再生器固有鍵(Kdev)に基づいてセーブデータ復号化鍵Ksavが生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。さらに、「プログラム使用制限なし」、かつ「記録再生器制限なし」の場合は、ステップS799において、システム共通鍵、例えばシステム署名鍵Ksysをセーブデータ復号化鍵Ksavとするか、あるいはシステム署名鍵Ksysに基づいてセーブデータ復号化鍵Ksavを生成する。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵Ksavとして使用してもよい。

【0581】

これらの復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて暗号化されたデータは、同一のコンテンツ固有鍵、記録再生器固有鍵に基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムが適用される。

【0582】

ステップS800では、上述のステップS796～S799のいずれかにおいて生成されたセーブデータ復号化鍵を用いて復号処理が実行され、復号セーブデータが記録再生器300において再生、実行される。

【0583】

この図80、82において示したセーブデータ格納、再生処理フローによれば、「プログラム使用制限する」の選択がなされたセーブデータはコンテンツ固有鍵によって暗号化、復号化処理が実行されるため、同一のコンテンツ固有鍵を持つコンテンツデータを使用する場合のみ復号して利用することが可能となる。また、「記録再生器制限する」の選択がなされたセーブデータは、記録再生器識別子によって暗号化、復号化処理が実行されるため、同一の記録再生器識別子を持つ記録再生器、すなわち同一の記録再生器によってのみ復号して利用することが

可能となる。従って、コンテンツ、記録再生器両者によって利用制限を設定することが可能となり、セーブデータのセキュリティをさらに高めることが可能となる。

【0584】

なお、図80、82においては、コンテンツ固有鍵、記録再生器固有鍵を用いたセーブデータ暗号化鍵、復号化鍵の生成構成を示したが、コンテンツ固有鍵の代わりにコンテンツ識別子、また記録再生器固有鍵の代わりに記録再生器識別子を用いて、これら識別子に基づいてセーブデータ暗号化鍵、復号化鍵の生成を実行する構成としてもよい。

【0585】

次に、図83～85を用いてユーザの入力したパスワードに基づいてセーブデータの暗号化鍵、復号化鍵を生成する構成について説明する。

【0586】

図83はユーザの入力したパスワードに基づいてセーブデータの暗号化鍵を生成して記録デバイスに格納する処理フローである。

【0587】

ステップS821は、コンテンツデータからコンテンツ識別子を読み出す処理であり、前述の各処理と同様である。ステップS822は、ユーザによるプログラム使用制限の設定を行なうか否かを決定するステップである。本構成において設定されるデータ管理ファイルは、例えば図84に示す構成を持つ。

【0588】

図84に示すように、データは、データ番号、コンテンツ識別子、記録再生器識別子、さらにユーザによるプログラム使用制限情報が含まれる。「ユーザによるプログラム使用制限情報」はプログラムを使用するユーザを制限するかしないかを設定する項目である。

【0589】

図83における処理フローにおけるステップS822において使用制限するの設定がなされると、ステップS823においてユーザパスワードの入力がなされる。この入力、図2に示す例えばキーボード等の入力手段から入力される。

【0590】

入力されたパスワードは、メインCPU106、制御部301の制御のもとに暗号処理部302に出力され、ステップS824における処理、すなわち入力ユーザパスワードに基づくセーブデータ暗号化鍵Ksavが生成される。セーブデータ暗号化鍵Ksav生成処理としては、例えばパスワード自体を暗号化鍵Ksavとしてもよいし、あるいは記録再生器のマスタ鍵MKxを用いて、セーブデータ暗号化鍵Ksav=DES(MKx, パスワード)によって生成してもよい。また、パスワードを入力として一方向性関数を適用して、その出力に基づいて暗号化鍵を生成してもよい。

【0591】

ステップS822におけるユーザ制限がNoとされている場合は、ステップS828において、記録再生器300のシステム共通鍵に基づいてセーブデータ暗号化鍵が生成される。

【0592】

さらに、ステップS825でステップS824、またはステップS828で生成したセーブデータ暗号化鍵Ksavを用いてセーブデータの暗号化処理がなされ、ステップS826において暗号化処理のなされたセーブデータが記録デバイスに格納される。

【0593】

さらに、ステップS827において、図84のデータ管理ファイルにステップS822で設定したユーザによるプログラム使用制限情報が、コンテンツ識別子と記録再生器識別子に対応付けられて書き込まれる。

【0594】

図85は、図83の処理によって格納されたセーブデータの再生処理フローを示した図である。ステップS831において、コンテンツデータからコンテンツ識別子を読み出し、ステップS832において図84に示したデータ管理ファイルからコンテンツ識別子、ユーザによるプログラム使用制限情報を読み出す。

【0595】

ステップS833において、データ管理ファイル中のデータに基づく判定を実

行し、「ユーザによるプログラム使用制限する」が設定されている場合は、ステップS834において、パスワード入力を求め、ステップS835において、入力パスワードに基づく復号化鍵を生成する。この復号化鍵生成処理は、暗号化鍵生成処理に対応する処理アルゴリズムが適用され、あるパスワードに基づいて暗号化されたデータは、同一のパスワードに基づいて生成された復号鍵によって復号可能なものとなる復号化鍵生成アルゴリズムに設定される。

【0596】

ステップS833の判定がユーザによるプログラム使用制限なしの場合は、ステップS837において記録再生器300の内部メモリに格納されたシステム共通鍵、例えばシステム署名鍵K_{sys}を用いてセーブデータ復号鍵K_{save}が生成される。または、別途、記録再生器300の内部メモリ307内に保存しておいた、他の鍵とは別の暗号鍵をセーブデータ暗号鍵K_{save}として使用してもよい。

【0597】

ステップS836では、ステップS835、ステップS837のいずれかにおいて生成された復号化鍵K_{save}を用いて記録デバイスに格納されたセーブデータの復号が実行され、ステップS836において記録再生器においてセーブデータの再生、実行がなされる。

【0598】

図83、図85において示したセーブデータ格納、再生処理フローによれば、「ユーザによるプログラム使用制限する」の選択がなされたセーブデータはユーザ入力パスワードに基づく鍵によって暗号化、復号化処理が実行されるため、同一のパスワードを入力した場合のみ復号して利用することが可能となり、セーブデータのセキュリティを高めることが可能となる。

【0599】

以上、いくつかのセーブデータの格納処理、再生処理態様について説明してきたが、上述した処理を融合した処理、例えばパスワードと、記録再生器識別子、コンテンツ識別子等を任意に組み合わせて使用してセーブデータ暗号化鍵、復号化鍵を生成する態様も可能である。

【0600】

(17) 不正機器の排除(リボケーション)構成

すでに説明してきたように、本発明のデータ処理装置においては、メディア500(図3参照)、通信手段600から提供される様々なコンテンツデータを記録再生器300において、認証、暗号化処理等を実行し、記録デバイスに格納する構成によって提供コンテンツのセキュリティを高めるとともに、また、正当な利用者のみが利用可能とする構成を持つ。

【0601】

上述の説明から理解されるように、入力コンテンツは、記録再生器300の暗号処理部302に構成される内部メモリ307に格納された様々な署名鍵、マスター鍵、チェック値生成鍵(図18参照)を用いて、認証処理、暗号化処理、復号化処理がなされる。この鍵情報を格納する内部メモリ307は、先に説明したように、基本的に外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧またはノイズ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性とした構成とされるのが望ましいが、万が一内部メモリの不正な読み取りが実行され、これらの鍵データ等が流出し、正規なライセンスのされていない記録再生器にコピーされた場合、コピーされた鍵情報によって不正なコンテンツ利用がなされる可能性がある。

【0602】

ここでは、これらの不正コピーによる鍵の複製によるコンテンツの不正利用を防止する構成について説明する。

【0603】

図86に、本構成「(17)不正機器の排除構成」を説明するブロック図を示す。記録再生器300は、前述の図2、3に示す記録再生器と同様であり、内部メモリを有し、先に説明した(図18)各種の鍵データ、さらに、記録再生器識別子を有している。なお、ここでは、第三者によって複製されている記録再生器識別子、鍵データ等は図3に示す内部メモリ307に格納されるとは限らず、図86に示す記録再生器300の鍵データ等は、暗号処理部302(図2、3参照

）によってアクセス可能なメモリ部にまとめて、あるいは分散して格納されている構成であるとする。

【0604】

不正機器の排除構成を実現するため、コンテンツデータのヘッダ部の不正な記録再生器識別子リストを記憶した構成とした。図86に示すように、コンテンツデータには、不正な記録再生器識別子（IDdev）リストとしてのリボケーション(Revocation)リストを保有している。さらに、リボケーションリストの改竄チェック用のリストチェック値ICVrevを設けている。不正な記録再生器識別子（IDdev）リストは、コンテンツ提供者、または管理者が、例えば不正コピーの流通状態等から判明した不正な記録再生器の識別子IDdevをリスト化したものである。このリボケーションリストは例えば配送鍵Kdisによって暗号化されて格納してもよい。記録再生器による復号処理については、例えば先の図22のコンテンツダウンロード処理の態様と同様である。

【0605】

なお、ここでは、理解を容易にするため、リボケーションリストを単独のデータとして図86のコンテンツデータ中に示してあるが、例えば先に説明したコンテンツデータのヘッダ部の構成要素である取扱方針（例えば図32～35参照）中にリボケーションリストを含ませてもよい。この場合は、先に説明したチェック値ICVaによってリボケーションリストを含む取扱方針データの改竄チェックがなされる。リボケーションリストが取扱方針中に含まれる場合は、チェック値A：ICVaのチェックによって代替され、記録再生器内のチェック値A生成鍵Kicvaが利用され、チェック値生成鍵Kicvrevを格納する必要はない。

【0606】

リボケーションリストを単独のデータとしてコンテンツデータ中に含ませる場合は、リボケーションリストの改竄チェック用のリストチェック値ICVrevによるリボケーションリストのチェックを実行するとともに、リストチェック値ICVrevとコンテンツデータ中の他の部分チェック値とから中間チェック値を生成して中間チェック値の検証処理を行なう構成とする。

【0607】

リボケーションリストの改竄チェック用のリストチェック値ICVrevによるリボケーションリストのチェック手法は、前述の図23、図24等で説明したICVa、ICVb等のチェック値生成処理と同様の方法で実行可能である。すなわち、記録再生器暗号処理部302の内部メモリ307に保存したチェック値生成鍵Kicvrevを鍵とし、コンテンツデータ中に含まれるリボケーションリストをメッセージとして図23、図24等で説明したICV計算方法に従って計算される。計算したチェック値ICVrev' とヘッダ (Header) 内に格納されたチェック値: ICVrevを比較し、一致していた場合には、改竄が無いと判定する。

【0608】

リストチェック値ICVrevを含む中間チェック値は、例えば、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されている総チェック値生成鍵Kicvtを鍵とし、検証したHeader内のチェック値A、チェック値B、リストチェック値ICVrev、さらにフォーマットに応じてコンテンツチェック値を加えたメッセージ列に図7他で説明したICV計算方法を適用して生成する。

【0609】

これらのリボケーションリスト、リストチェック値は、DVD、CD等のメディア500、通信手段600を介して、あるいはメモリカード等の記録デバイス400を介して記録再生器300に提供される。ここで記録再生器300は、正当な鍵データを保有する記録再生器である場合と、不正に複製された識別子IDを有する場合とがある。

【0610】

このような構成における不正な記録再生器の排除処理の処理フローを図87および図88に示す。図87は、DVD、CD等のメディア500、あるいは通信手段600からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フローであり、図88は、メモリカード等の記録デバイス400からコンテンツが提供される場合の不正記録再生器排除（リボケーション）処理フロ

一である。

【0611】

まず、図87の処理フローについて説明する。ステップ901は、メディアを装着して、コンテンツの提供、すなわち再生処理あるいはダウンロードの要求を行なうステップである。この図87に示す処理は、例えば記録再生器にDVD等のメディアを装着してダウンロード処理等を実行する前のステップとして実行される。ダウンロード処理については、先に図22を用いて説明している通りであり、図22の処理フローの実行の前ステップとして、あるいは図22の処理フロー中に挿入される処理としてこの図87の処理が実行される。

【0612】

記録再生器300がネットワーク等の通信手段を介してコンテンツ提供を受ける場合は、ステップS911においてコンテンツ配信サービス側との通信セッションを確立し、その後、ステップS902へ進む。

【0613】

ステップS902では、コンテンツデータのヘッダ部からリボケーションリスト(図86参照)を取得する。このリスト取得処理は、コンテンツがメディア内にある場合は、図3に示す制御部301が読取部304を介してメディアから読み出し、コンテンツが通信手段からである場合は、図3に示す制御部301が通信部305を介してコンテンツ配信側から受信する。

【0614】

次にステップS903において、制御部301は、暗号処理部302にメディア500または通信手段600から取得したリボケーションリストを暗号処理部302に渡し、チェック値生成処理を実行させる。記録再生器300は、内部にリボケーションチェック値生成鍵*K_{icv-rev}*を有し、受領したリボケーションリストをメッセージとしてリボケーションチェック値生成鍵*K_{icv-rev}*を適用して、例えば図23、図24等で説明したICV計算方法に従ってチェック値*ICV-rev'*を計算し、計算結果とコンテンツデータのヘッダ(Header)内に格納されたチェック値：*ICV-rev*を比較し、一致していた場合には改竄が無い(ステップS904でYes)と判定する。一致しない場合は、改

竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。

【0615】

次に、ステップS905において、記録再生器暗号処理部302の制御部306は、記録再生器暗号処理部302の暗号／復号化部308に総チェック値ICVt'の計算をさせる。総チェック値ICVt'は、図25に示すように、記録再生器暗号処理部302の内部メモリ307に保存されているシステム署名鍵Ksysを鍵とし、中間チェック値をDESで暗号化して生成する。なお、各部分チェック値、例えばICVa、ICVb等の検証処理は、この図87に示す処理フロー中では省略してあるが、先に説明した図39～図45の処理フローと同様の各データフォーマットに応じた部分チェック値の検証が行なわれる。

【0616】

次に、ステップS906において、生成した総チェック値ICVt'とヘッダ(Header)内のICVtを比較し、一致していた場合(ステップS906でYes)には、ステップS907へ進む。一致しない場合は、改竄されていると判定され、ステップS909に進み処理エラーとして処理を終了する。

【0617】

先に説明したように、総チェック値ICVtは、ICVa、ICVb、さらに、データフォーマットに応じて各コンテンツブロックのチェック値等、コンテンツデータに含まれる部分チェック値全体をチェックするものであるが、ここでは、これらの部分チェック値にさらに、リボケーションリストの改竄チェック用のリストチェック値ICVrevを部分チェック値として加えて、これら全ての改竄を検証する。上述の処理によって生成された総チェック値がヘッダ(Header)内に格納されたチェック値：ICVtと一致した場合には、ICVa、ICVb、各コンテンツブロックのチェック値、およびリストチェック値ICVrev全ての改竄はないと判断される。

【0618】

さらにステップS907では、改竄無しと判定されたりボケーションリストと、自己の記録再生器300に格納された記録再生器識別子(IDdev)との比

較がなされる。

【0619】

コンテンツデータから読み出された不正な記録再生器識別子ID devのリストに自己の記録再生器の識別子ID devが含まれている場合は、その記録再生器300は、不正に複製された鍵データを有していると判定され、ステップS909に進み、以後の手続きは中止される。例えば図22のコンテンツダウンロード処理の手続きの実行を不可能とする。

【0620】

ステップS907において、不正な記録再生器識別子ID devのリストに自己の記録再生器の識別子ID devが含まれていないと判定された場合には、その記録再生器300は、正当な鍵データを有していると判定され、ステップS908に進み、以後の手続き、例えば、プログラム実行処理、あるいは図22等のコンテンツダウンロード処理等が実行可能となる。

【0621】

図88は、メモ리카ード等の記録デバイス400に格納したコンテンツデータを再生する場合の処理を示す。先に説明したように、メモ리카ード等の記録デバイス400と記録再生器300は、図20で説明した相互認証処理（ステップS921）が実行される。ステップS922において、相互認証OKである場合にのみ、ステップS923以降の処理に進み、相互認証に失敗した場合は、ステップS930のエラーとなり、以降の処理は実行されない。

【0622】

ステップS923では、コンテンツデータのヘッダ部からリボケーションリスト(図86参照)を取得する。以降のステップS924～S930の処理は、先の図87における対応処理と同様の処理である。すなわち、リストチェック値によるリストの検証(S924, S925)、総チェック値による検証(S926, S927)、リストのエントリと自己の記録再生器識別子ID devとの比較(S928)を実行し、コンテンツデータから読み出された不正な記録再生器識別子ID devのリストに自己の記録再生器の識別子ID devが含まれている場合は、その記録再生器300は、不正に複製された鍵データを有していると判定

され、ステップ S 9 3 0 に進み、以後の手続きは中止される。例えば図 2 8 に示すコンテンツの再生処理を実行不可能とする。一方、不正な記録再生器識別子 I D d e v のリストに自己の記録再生器の識別子 I D d e v が含まれていないと判定された場合には、その記録再生器 3 0 0 は、正当な鍵データを有していると判定され、ステップ S 9 2 9 に進み、以後の手続きが実行可能となる。

【 0 6 2 3 】

このように、本発明のデータ処理装置においては、コンテンツ提供者、または管理者が提供するコンテンツに併せて不正な記録再生器を識別するデータ、すなわち不正な記録再生器識別子 I D d e v をリスト化したリボケーションリストをコンテンツデータのヘッダ部の構成データとして含ませて記録再生器利用者に提供し、記録再生器利用者は、記録再生器によるコンテンツの利用に先立って、自己の記録再生器のメモリに格納された記録再生器識別子 I D d e v と、リストの識別子との照合を実行して一致するデータが存在した場合には、以後の処理を実行させない構成としたので鍵データを複製してメモリに格納した不正な記録再生器によるコンテンツ利用を排除することが可能となる。

【 0 6 2 4 】

(1 8) セキュアチップ構成および製造方法

先に説明したように、記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7、あるいは記録デバイス 4 0 0 の内部メモリ 4 0 5 は、暗号鍵などの重要な情報を保持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、記録再生器暗号処理部 3 0 2、記録デバイス暗号処理部 4 0 1 は、例えば外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧またはノット周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【 0 6 2 5 】

しかしながら、上述の説明で理解されるように、例えば記録再生器暗号処理部 3 0 2 の内部メモリ 3 0 7 には記録再生器署名鍵 K d e v 等の記録再生器毎に異なるデータを書き込むことが必要となる。また、チップ内の不揮発性の記憶領域

、例えばフラッシュメモリ、FeRAM等にチップ毎の個別情報、例えば識別情報（ID）や暗号鍵情報を書き込んだ後、例えば製品出荷後におけるデータの再書き込み、読み出しを困難とすることが必要となる。

【0626】

従来の書き込みデータの読み出し、再書き込み処理を困難とするための手法には、例えばデータ書き込みのコマンドプロトコルを秘密にする。あるいは、チップ上のデータ書き込みコマンドを受け付ける信号線と、製品化した後に利用される通信用の信号線を分離して構成し、基板上のチップに直接信号を送らない限りデータ書き込みコマンドが有効とならないようにする等の手法がある。

【0627】

しかしながら、このような従来手法を採用しても、記憶素子の専門知識を有するものにとっては、回路を駆動させる設備と技術があれば、チップのデータ書き込み領域に対する信号出力が可能であり、また、たとえデータ書き込みのコマンドプロトコルが秘密であったとしても、プロトコルの解析可能性は常に存在する。

【0628】

このような、秘密データの改変可能性を保持した暗号処理データの格納素子を流通させることは、暗号処理システム全体を脅かす結果となる。また、データの読み出しを防止するために、データ読み出しコマンド自体を実装しない構成とすることも可能であるが、その場合、正規のデータ書き込みを実行した場合であっても、メモリに対するデータ書き込みが実際に行われたか否かを確認したり、書き込まれたデータが正確に書き込まれているか否かを判定することが不可能となり、不良なデータ書き込みの行われたチップが供給される可能性が発生する。

【0629】

これらの従来技術に鑑み、ここでは、例えばフラッシュメモリ、FeRAM等の不揮発性メモリに正確なデータ書き込みを可能とするとともに、データの読み出しを困難にするセキュアチップ構成およびセキュアチップ製造方法を提供する。

【0630】

図 8 9 に、例えば、前述の記録再生器暗号処理部 3 0 2 または記録デバイス 4 0 0 の暗号処理部 4 0 1 に適用可能なセキュリティチップ構成を示す。図 8 9 (A) はチップの製造過程、すなわちデータの書き込み過程におけるセキュリティチップ構成を示し、図 8 9 (B) は、データを書き込んだセキュリティチップを搭載した製品の構成例、例えば記録再生器 3 0 0、記録デバイス 4 0 0 の例を示す。

【 0 6 3 1 】

製造過程にあるセキュリティチップは、処理部 8 0 0 1 にモード指定用信号線 8 0 0 3、および各種コマンド信号線 8 0 0 4 が接続され、処理部 8 0 0 1 は、モード指定用信号線 8 0 0 3 で設定されたモード、例えばデータ書き込みモードまたはデータ読み出しモードに応じて不揮発性メモリである記憶部 8 0 0 2 へのデータ書き込み処理、または記憶部 8 0 0 2 からのデータ読み出し処理を実行する。

【 0 6 3 2 】

一方、図 8 9 (B) のセキュリティチップ搭載製品においては、セキュリティチップと外部接続インタフェース、周辺機器、他の素子等とが汎用信号線で接続されるが、モード信号線 8 0 0 3 は、非接続状態とされる。具体的な処理は、例えばモード信号線 8 0 0 3 をグランド接続する、V c c に釣り上げる、信号線をカットする、あるいは絶縁体樹脂で封印する等である。このような処理により、製品出荷後は、セキュリティチップのモード信号線に対するアクセスが困難になり、外部からチップのデータを読み出したり書き込みを行なったりすることの困難性を高めることができる。

【 0 6 3 3 】

さらに、本構成のセキュリティチップ 8 0 0 0 は、データの記憶部 8 0 0 2 に対する書き込み処理、および記憶部 8 0 0 2 に書き込まれたデータの読み出し処理を困難にする構成を持ち、たとえ第三者がモード信号線 8 0 0 3 のアクセスに成功した場合であっても不正なデータ書き込み、読み出しを防止可能である。図 9 0 に本構成を有するセキュリティチップにおけるデータ書き込みまたは読み出し処理フローを示す。

【 0 6 3 4 】

ステップ S 9 5 1 は、モード信号線 8 0 0 3 をデータ書き込みモードまたはデータ読み出しモードに設定するステップである。

【 0 6 3 5 】

ステップ S 9 5 2 は、チップから認証用情報を取り出すステップである。本構成のセキュリティチップには、例えばワイヤ (Wire)、マスク ROM 構成により、予めパスワード、暗号技術における認証処理用の鍵情報等、認証処理に必要な情報が格納される。ステップ S 9 5 2 は、この認証情報を読み出して認証処理を実行する。例えば正規なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証 OK (ステップ S 9 5 3 において Yes) の結果が得られるが、不正なデータ書き込み治具、データ読み出し装置を汎用信号線に接続して認証処理を実行した場合には、認証に失敗 (ステップ S 9 5 3 において No) し、その時点で処理が中止される。認証処理は、例えば先に説明した図 1 3 の相互認証処理手続きに従って実行可能である。図 8 9 に示す処理部 8 0 0 1 は、これらの認証処理を実行可能な構成を有する。これは、例えば先に説明した図 2 9 に示す記録デバイス 4 0 0 の暗号処理部 4 0 1 の制御部 4 0 3 に組み込まれたコマンドレジスタと同様の構成により実現可能である。例えば図 8 9 のチップの処理部は、図 2 9 に示す記録デバイス 4 0 0 の暗号処理部 4 0 1 の制御部 4 0 3 に組み込まれたコマンドレジスタと同様の構成を持ち、各種コマンド信号線 8 0 0 4 に接続された機器から所定のコマンド No が入力されると、対応する処理を実行し、認証処理シーケンスを実行することが可能となる。

【 0 6 3 6 】

処理部 8 0 0 1 は認証処理において認証がなされた場合にのみ、データの書き込みコマンド、またはデータの読み出しコマンドを受け付けてデータの書き込み処理 (ステップ S 9 5 5)、またはデータの読み出し処理 (ステップ S 9 5 6) を実行する。

【 0 6 3 7 】

このように本構成のセキュリティチップにおいては、データの書き込み時、読

み出し時に認証処理を実行する構成としたので、正当な権利を持たない第三者によるセキュリティチップの記憶部からデータの読み出し、または記憶部へのデータ書き込みを防止することができる。

【0638】

次に、さらに、セキュリティの高い素子構成とした実施例を図91に示す。この例では、セキュリティチップの記憶部8200が2つの領域に分離され、一方はデータの読み書きが可能な読み出し書き込み併用領域(RW: ReadWrite領域)8201であり、他方はデータの書き込みのみが可能な書き込み専用領域(WO: WriteOnly領域)8202である。

【0639】

この構成において、書き込み専用領域(WO: WriteOnly領域)8202には、暗号鍵データ、識別子データ等のセキュリティ要請の高いデータを書き込み、一方セキュリティ度のさほど高くない、例えばチェック用のデータ等を読み出し書き込み併用領域(RW: ReadWrite領域)8201に書き込む。

【0640】

処理部8001は、読み出し書き込み併用領域(RW: ReadWrite領域)8201からのデータ読み出し処理は、前述の図90で説明した認証処理を伴うデータ読み出し処理を実行する。しかし、データ書き込み処理は、図92のフローに従って実行する。

【0641】

図92のステップS961は、モード信号線8003を書き込みモードに設定するステップであり、ステップ962では、先の図90で説明したと同様の認証処理を実行する。認証処理で認証がなされると、ステップS963に進み、コマンド信号線8004を介して、書き込み専用(WO)領域8202にセキュリティの高い鍵データ等の情報の書き込み、読み出し書き込み併用領域(RW: ReadWrite領域)8201にセキュリティ度のさほど高くない、例えばチェック用データ書き込むコマンドを処理部8001に対して出力する。

【0642】

ステップS964ではコマンドを受領した処理部8001が、コマンドに応じたデータ書き込み処理をそれぞれ書き込み専用(WO)領域8202、読み出し書き込み併用領域(RW:ReadWrite領域)8201に対して実行する。

【0643】

また、書き込み専用(WO)領域8202に書き込まれたデータの検証処理フローを図93に示す。

【0644】

図93のステップS971は、処理部8001において、書き込み専用(WO)領域8202に書き込まれたデータに基づく暗号処理を実行させる。これらの実行構成は、先の認証処理実行構成と同様、コマンドレジスタに格納された暗号処理シーケンスを順次実行する構成によって実現される。また、処理部8001において実行される暗号処理アルゴリズムは特に限定されるものではなく、例えば先に説明したDESアルゴリズムを実行する構成とすることができる。

【0645】

次に、ステップS972で、セキュリティチップに接続された検証装置が処理部8001から暗号処理結果を受信する。次に、ステップS973において、先に記憶部に書き込み処理を行なった正規な書き込みデータに対して処理部8001において実行されたアルゴリズムと同様の暗号化処理を適用して得た結果と、処理部8001からの暗号化結果とを比較する。

【0646】

比較した結果が同一であれば、書き込み専用(WO)領域8202に書き込まれたデータは正しいことが検証される。

【0647】

この構成では、認証処理が破られて読み出しコマンドが万が一実行可能となっても、データの読み出し可能領域は、読み出し書き込み併用領域(RW:ReadWrite領域)8201に限定され、書き込み専用(WO)領域8202に書き込まれたデータの読み出しは、不可能であり、さらにセキュリティの高い構成となる。また、全く読み出しを不可能としたチップと異なり、読み出し書き込み併用領域(RW:ReadWrite領域)8201が構成されているのでメモ

リアクセスの正否チェックが可能である。

【 0 6 4 8 】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。また、上記した実施例ではコンテンツの記録、再生を可能な記録再生器を例にして説明してきたが、データ記録のみ、データ再生のみ可能な装置においても本発明の構成は適用可能なものであり、本発明はパーソナルコンピュータ、ゲーム機器、その他の各種データ処理装置一般において実施可能なものである。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【 0 6 4 9 】

【発明の効果】

上述したように、本発明のデータ処理装置、データ処理システム、およびデータ処理方法においては、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の暗号処理を実行するために必要となる個別鍵を記憶部に格納せず、これらの個別鍵を生成するためのマスター鍵を記憶部に格納した構成を持ち、データ処理装置における暗号処理部が、暗号鍵、認証鍵等の個別鍵を必要に応じて、それらの個別鍵に対応するマスター鍵を記憶部から取り出して、取り出したマスター鍵と、装置またはデータの識別データに基づいて、例えばDESアルゴリズムを適用した暗号処理を実行して、暗号鍵、認証鍵等の個別鍵を生成する構成としたので、個別鍵自体が記憶部から漏洩する可能性がなく、個別鍵を得るためには、個別鍵生成アルゴリズムと、マスター鍵の双方の情報、さらに装置またはデータの識別データ等、複数の情報が必要となり、暗号処理システムのセキュリティを高めることが可能となる。また、個別鍵が何らかの理由により漏洩したした場合でも、その被害の範囲は個別鍵の範囲に限定されるため、システム前名対の崩壊にはつながらないといえる。

【 0 6 5 0 】

さらに、本発明のデータ処理装置、データ処理システム、およびデータ処理方

法によれば、装置またはデータの識別データに基づいて、個別鍵を逐次生成する構成であるので、個々の装置に適用する鍵のリストを管理装置において保持する必要がなく、セキュリティが高まると同時にシステム管理も容易になる。

【図面の簡単な説明】

【図 1】

従来のデータ処理システムの構成を示す図である。

【図 2】

本発明の適用されるデータ処理装置の構成を示す図である。

【図 3】

本発明の適用されるデータ処理装置の構成を示す図である。

【図 4】

メディア上、通信路上におけるコンテンツデータのデータフォーマットを示す図である。

【図 5】

コンテンツデータ中のヘッダに含まれる取扱方針を示す図である。

【図 6】

コンテンツデータ中のヘッダに含まれるブロック情報を示す図である。

【図 7】

DESを用いた電子署名生成方法を示す図である。

【図 8】

トリプルDESを用いた電子署名生成方法を示す図である。

【図 9】

トリプルDESの態様を説明する図である。

【図 10】

一部にトリプルDESを用いた電子署名生成方法を示す図である。

【図 11】

電子署名生成における処理フローを示す図である。

【図 12】

電子署名検証における処理フローを示す図である。

【図 1 3】

対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

【図 1 4】

公開鍵証明書を説明する図である。

【図 1 5】

非対称鍵暗号技術を用いた相互認証処理の処理シーケンスを説明する図である。

【図 1 6】

楕円曲線暗号を用いた暗号化処理の処理フローを示す図である。

【図 1 7】

楕円曲線暗号を用いた復号化処理の処理フローを示す図である。

【図 1 8】

記録再生器上のデータ保持状況を示す図である。

【図 1 9】

記録デバイス上のデータ保持状況を示す図である。

【図 2 0】

記録再生器と記録デバイスとの相互認証処理フローを示す図である。

【図 2 1】

記録再生器のマスタ鍵と記録デバイスの対応鍵ブロックとの関係を示す図である。

【図 2 2】

コンテンツのダウンロード処理における処理フローを示す図である。

【図 2 3】

チェック値 A : I C V a の生成方法を説明する図である。

【図 2 4】

チェック値 B : I C V b の生成方法を説明する図である。

【図 2 5】

総チェック値、記録再生器固有チェック値の生成方法を説明する図である。

【図 2 6】

記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝0）を示す図である。

【図 27】

記録デバイスに保存されたコンテンツデータのフォーマット（利用制限情報＝1）を示す図である。

【図 28】

コンテンツの再生処理における処理フローを示す図である。

【図 29】

記録デバイスにおけるコマンド実行方法について説明する図である。

【図 30】

記録デバイスにおけるコンテンツ格納処理におけるコマンド実行方法について説明する図である。

【図 31】

記録デバイスにおけるコンテンツ再生処理におけるコマンド実行方法について説明する図である。

【図 32】

コンテンツデータフォーマットのフォーマット・タイプ0の構成を説明する図である。

【図 33】

コンテンツデータフォーマットのフォーマット・タイプ1の構成を説明する図である。

【図 34】

コンテンツデータフォーマットのフォーマット・タイプ2の構成を説明する図である。

【図 35】

コンテンツデータフォーマットのフォーマット・タイプ3の構成を説明する図である。

【図 36】

フォーマット・タイプ0におけるコンテンツチェック値 I C V i の生成処理方

法を説明する図である。

【図37】

フォーマット・タイプ1におけるコンテンツチェック値ICViの生成処理方法を説明する図である。

【図38】

フォーマット・タイプ2, 3における総チェック値、記録再生器固有チェック値の生成処理方法を説明する図である。

【図39】

フォーマット・タイプ0, 1におけるコンテンツダウンロード処理の処理フローを示す図である。

【図40】

フォーマット・タイプ2におけるコンテンツダウンロード処理の処理フローを示す図である。

【図41】

フォーマット・タイプ3におけるコンテンツダウンロード処理の処理フローを示す図である。

【図42】

フォーマット・タイプ0におけるコンテンツ再生処理の処理フローを示す図である。

【図43】

フォーマット・タイプ1におけるコンテンツ再生処理の処理フローを示す図である。

【図44】

フォーマット・タイプ2におけるコンテンツ再生処理の処理フローを示す図である。

【図45】

フォーマット・タイプ3におけるコンテンツ再生処理の処理フローを示す図である。

【図46】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その1)である。

【図 4 7】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その2)である。

【図 4 8】

コンテンツ生成者と、コンテンツ検証者におけるチェック値の生成、検証方法を説明する図(その3)である。

【図 4 9】

マスタ鍵を用いて各種の鍵を個別に生成する方法について説明する図である。

【図 5 0】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図(例1)である。

【図 5 1】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図(例2)である。

【図 5 2】

マスタ鍵の使い分けにより、利用制限を実行する構成について説明する図である。

【図 5 3】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図(例3)である。

【図 5 4】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図(例4)である。

【図 5 5】

マスタ鍵を用いて各種の鍵を個別に生成する方法について、コンテンツプロバイダと、ユーザにおける処理例を示す図(例5)である。

【図 5 6】

トリプルDESを適用した暗号鍵をシングルDESアルゴリズムを用いて格納する処理フローを示す図である。

【図 5 7】

優先順位に基づくコンテンツ再生処理フロー（例 1）を示す図である。

【図 5 8】

優先順位に基づくコンテンツ再生処理フロー（例 2）を示す図である。

【図 5 9】

優先順位に基づくコンテンツ再生処理フロー（例 3）を示す図である。

【図 6 0】

コンテンツ再生処理における圧縮データの復号（伸長）処理を実行する構成について説明する図である。

【図 6 1】

コンテンツの構成例（例 1）を示す図である。

【図 6 2】

コンテンツの構成例 1 における再生処理フローを示す図である。

【図 6 3】

コンテンツの構成例（例 2）を示す図である。

【図 6 4】

コンテンツの構成例 2 における再生処理フローを示す図である。

【図 6 5】

コンテンツの構成例（例 3）を示す図である。

【図 6 6】

コンテンツの構成例 3 における再生処理フローを示す図である。

【図 6 7】

コンテンツの構成例（例 4）を示す図である。

【図 6 8】

コンテンツの構成例 4 における再生処理フローを示す図である。

【図 6 9】

セーブデータの生成、格納処理について説明する図である。

【図 70】

セーブデータの格納処理例(例1)に関する処理フローを示す図である。

【図 71】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例1)を示す図である。

【図 72】

セーブデータの再生処理例(例1)に関する処理フローを示す図である。

【図 73】

セーブデータの格納処理例(例2)に関する処理フローを示す図である。

【図 74】

セーブデータの再生処理例(例2)に関する処理フローを示す図である。

【図 75】

セーブデータの格納処理例(例3)に関する処理フローを示す図である。

【図 76】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例2)を示す図である。

【図 77】

セーブデータの再生処理例(例3)に関する処理フローを示す図である。

【図 78】

セーブデータの格納処理例(例4)に関する処理フローを示す図である。

【図 79】

セーブデータの再生処理例(例4)に関する処理フローを示す図である。

【図 80】

セーブデータの格納処理例(例5)に関する処理フローを示す図である。

【図 81】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例3)を示す図である。

【図 82】

セーブデータの再生処理例(例5)に関する処理フローを示す図である。

【図 8 3】

セーブデータの格納処理例(例 6)に関する処理フローを示す図である。

【図 8 4】

セーブデータの格納、再生処理において使用されるデータ管理ファイル構成(例 4)を示す図である。

【図 8 5】

セーブデータの再生処理例(例 6)に関する処理フローを示す図である。

【図 8 6】

コンテンツ不正利用者排除(リボケーション)構成を説明する図である。

【図 8 7】

コンテンツ不正利用者排除(リボケーション)の処理フロー(例 1)を示す図である。

【図 8 8】

コンテンツ不正利用者排除(リボケーション)の処理フロー(例 2)を示す図である。

【図 8 9】

セキュリティチップの構成(例 1)を説明する図である。

【図 9 0】

セキュリティチップの製造方法における処理フローを示す図である。

【図 9 1】

セキュリティチップの構成(例 2)を説明する図である。

【図 9 2】

セキュリティチップ(例 2)におけるデータ書き込み処理における処理フローを示す図である。

【図 9 3】

セキュリティチップ(例 2)における書き込みデータチェック処理における処理フローを示す図である。

【符号の説明】

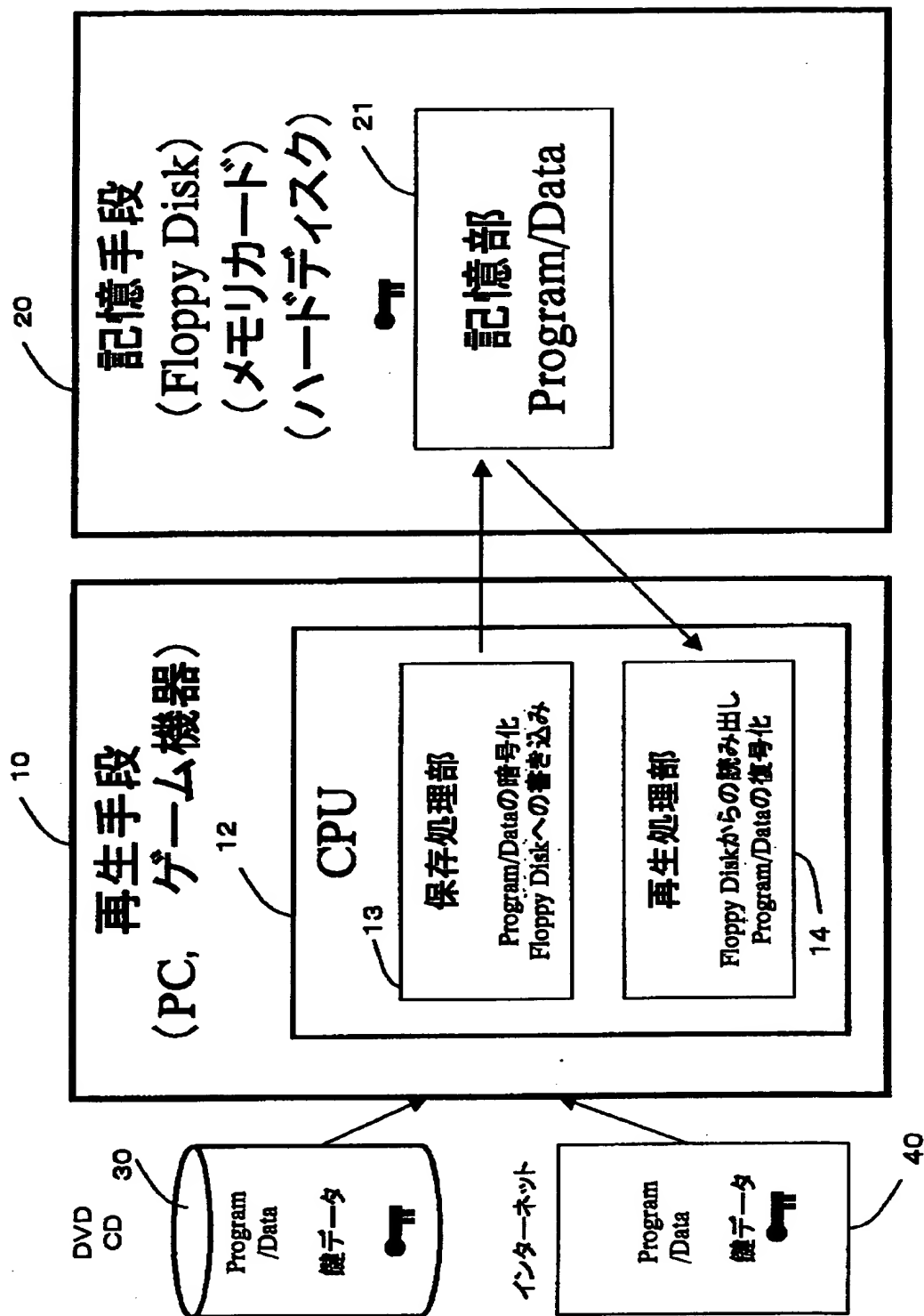
1 0 6 メイン CPU

1 0 7 R A M
 1 0 8 R O M
 1 0 9 A V 処理部
 1 1 0 入力処理部
 1 1 1 P I O
 1 1 2 S I O
 3 0 0 記録再生器
 3 0 1 制御部
 3 0 2 暗号処理部
 3 0 3 記録デバイスコントローラ
 3 0 4 読み取り部
 3 0 5 通信部
 3 0 6 制御部
 3 0 7 内部メモリ
 3 0 8 暗号／復号化部
 4 0 0 記録デバイス
 4 0 1 暗号処理部
 4 0 2 外部メモリ
 4 0 3 制御部
 4 0 4 通信部
 4 0 5 内部メモリ
 4 0 6 暗号／復号化部
 4 0 7 外部メモリ制御部
 5 0 0 メディア
 6 0 0 通信手段
 2 1 0 1, 2 1 0 2, 2 1 0 3 記録再生器
 2 1 0 4, 2 1 0 5, 2 1 0 6 記録デバイス
 2 9 0 1 コマンド番号管理部
 2 9 0 2 コマンドレジスタ

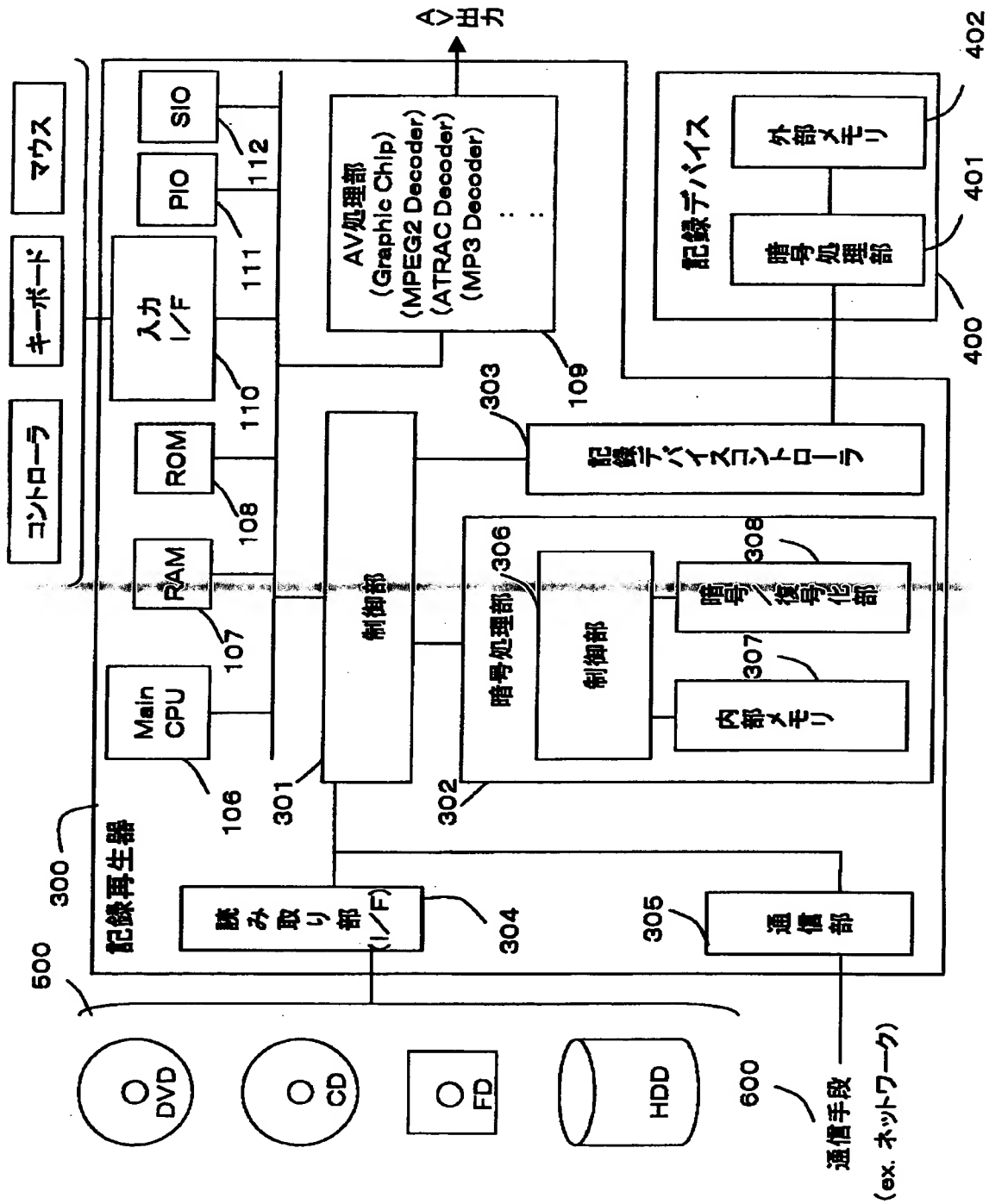
2903, 2904 認証フラグ
3001 スピーカ
3002 モニタ
3090 メモリ
3091 コンテンツ解析部
3092 データ記憶部
3093 プログラム記憶部
3094 圧縮伸長処理部
7701 コンテンツデータ
7702 リボケーションリスト
7703 リストチェック値
8000 セキュリティチップ
8001 処理部
8002 記憶部
~~8003 モード信号線~~
8004 コマンド信号線
8201 読み出し書き込み併用領域
8202 書き込み専用領域

【書類名】 図面

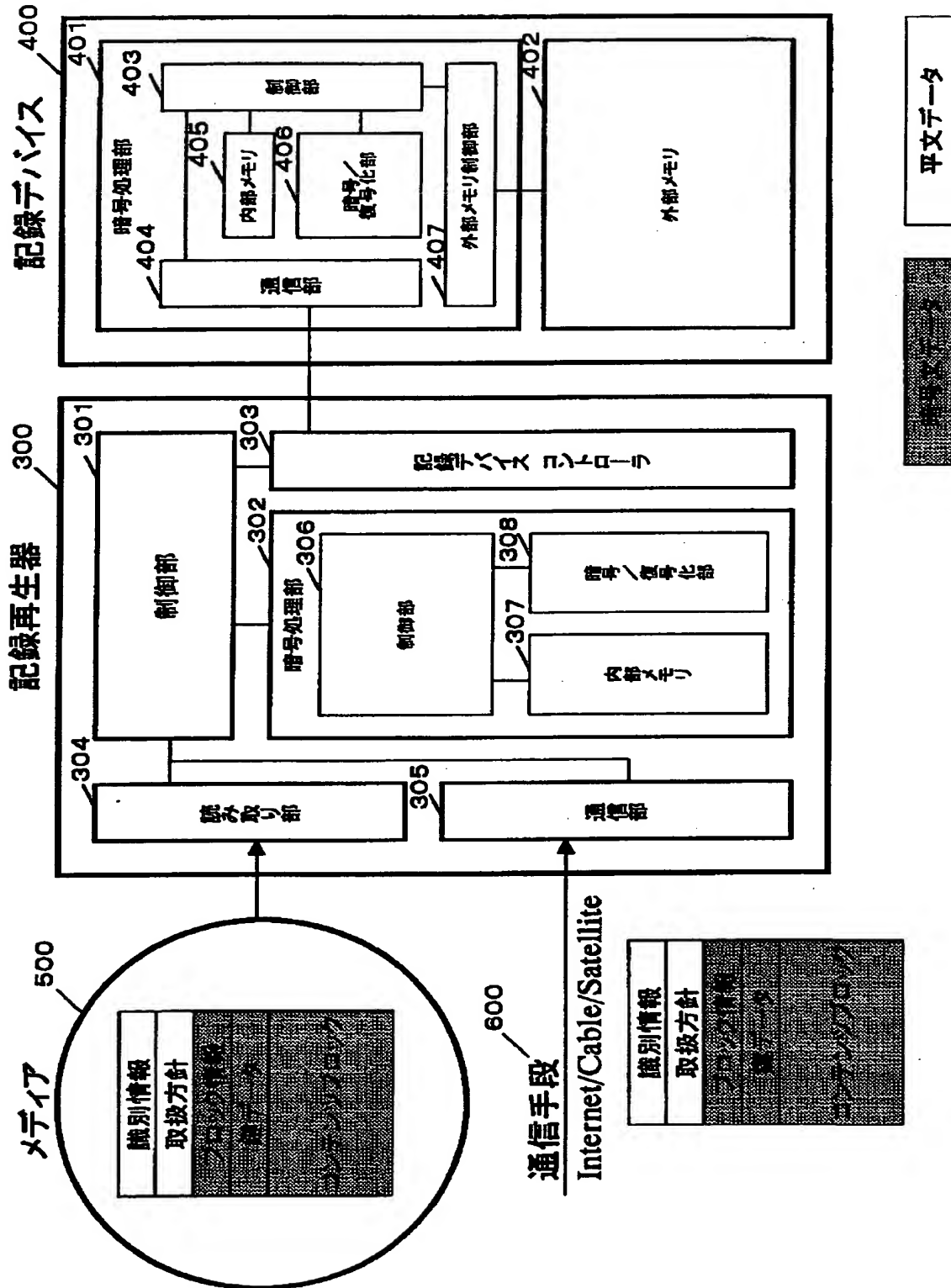
【図 1】



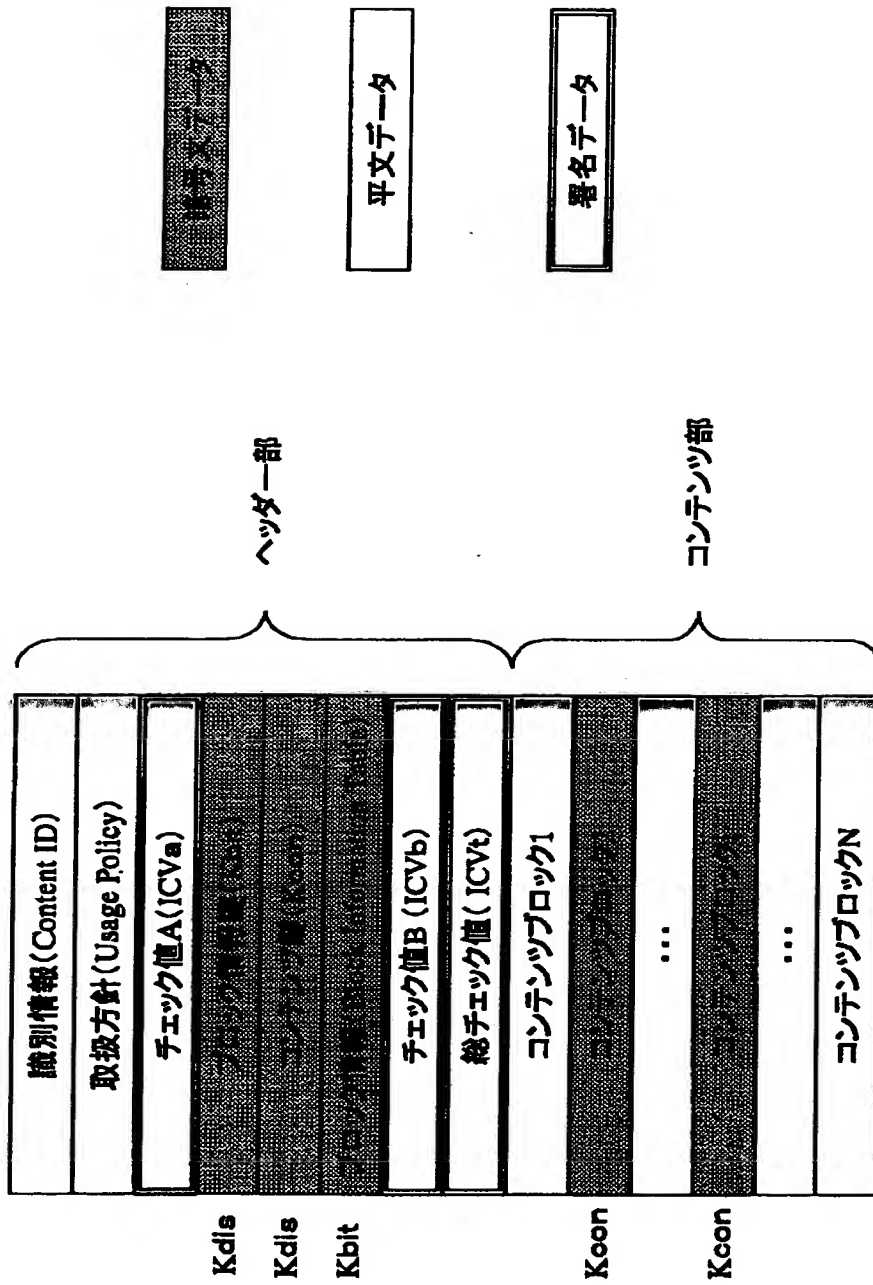
【図2】



【図 3】



【図4】



メディア上及び通信路上のデータフォーマット

【図 5】

| |
|--------------------------------|
| ヘッダーサイズ(Header Length) |
| コンテンツサイズ(Content Length) |
| フォーマットバージョン(Format Version) |
| フォーマットタイプ(Format Type) |
| コンテンツタイプ(Content Type) |
| 起動優先順位情報(Operation Priority) |
| 利用制限情報(Localization Field) |
| 複製制限情報(Copy Permission) |
| 移動制限情報(Move Permission) |
| 暗号アルゴリズム(Encryption Algorithm) |
| 暗号化モード(Encryption Mode) |
| 検証方法(Integrity Check Method) |

取扱方針

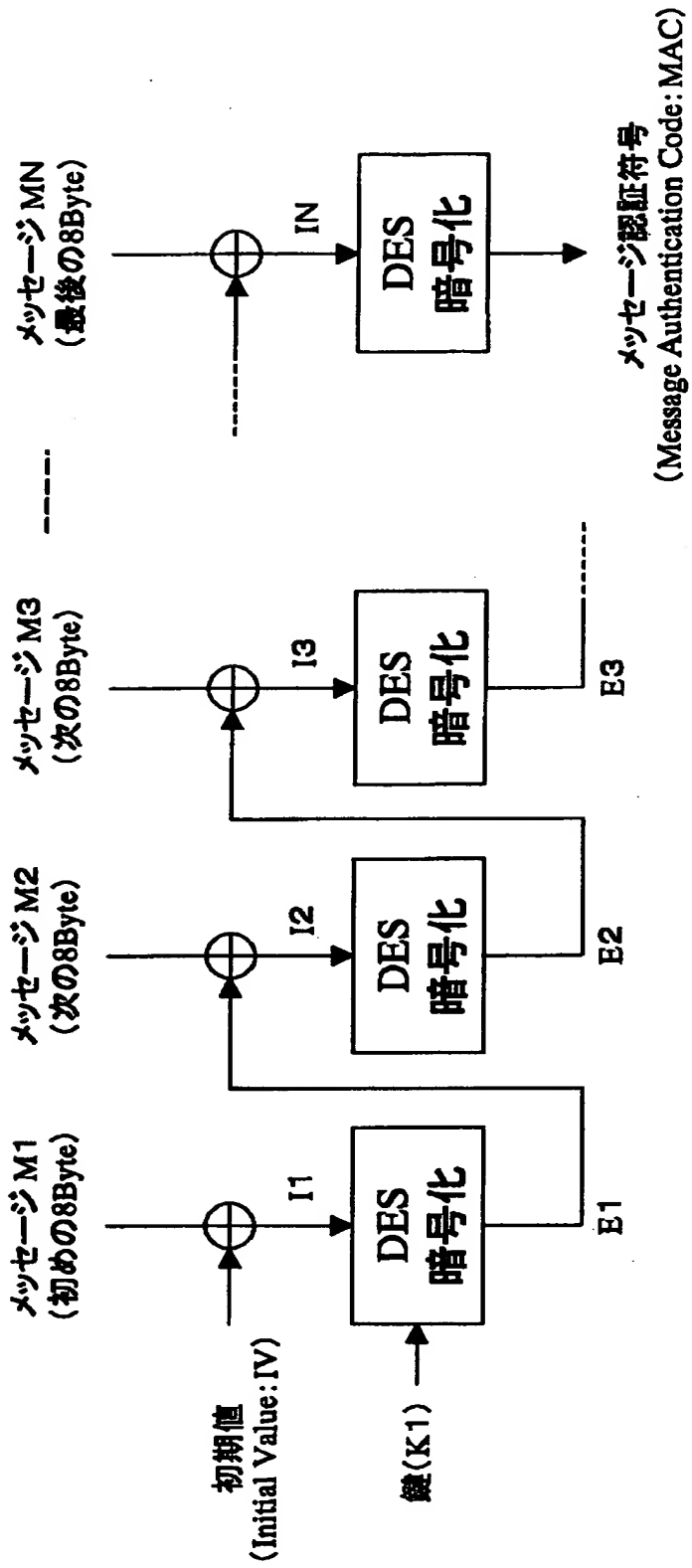
【図 6】

Kbit

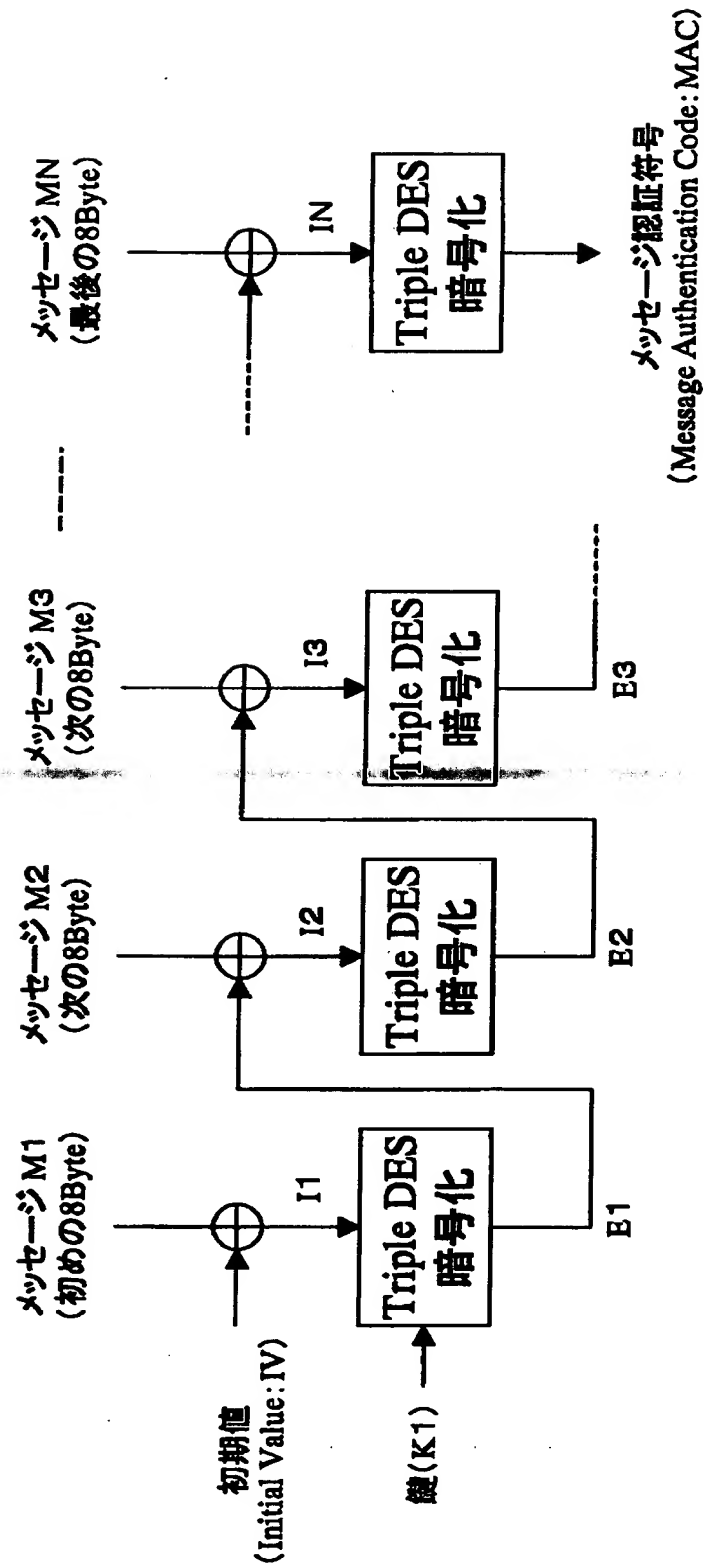
| | |
|--------------------------|-------------------------|
| コンテンツブロック数(Block Number) | |
| ブロック 1 | ブロックサイズ(Block Length) |
| | 暗号化フラグ(Encryption Flag) |
| | 検証対象フラグ(ICV Flag) |
| | コンテンツチェック値(ICV1) |
| ... | |
| ブロック N | ブロックサイズ(Block Length) |
| | 暗号化フラグ(Encryption Flag) |
| | 検証対象フラグ(ICV Flag) |
| | コンテンツチェック値(ICVN) |

ブロック情報

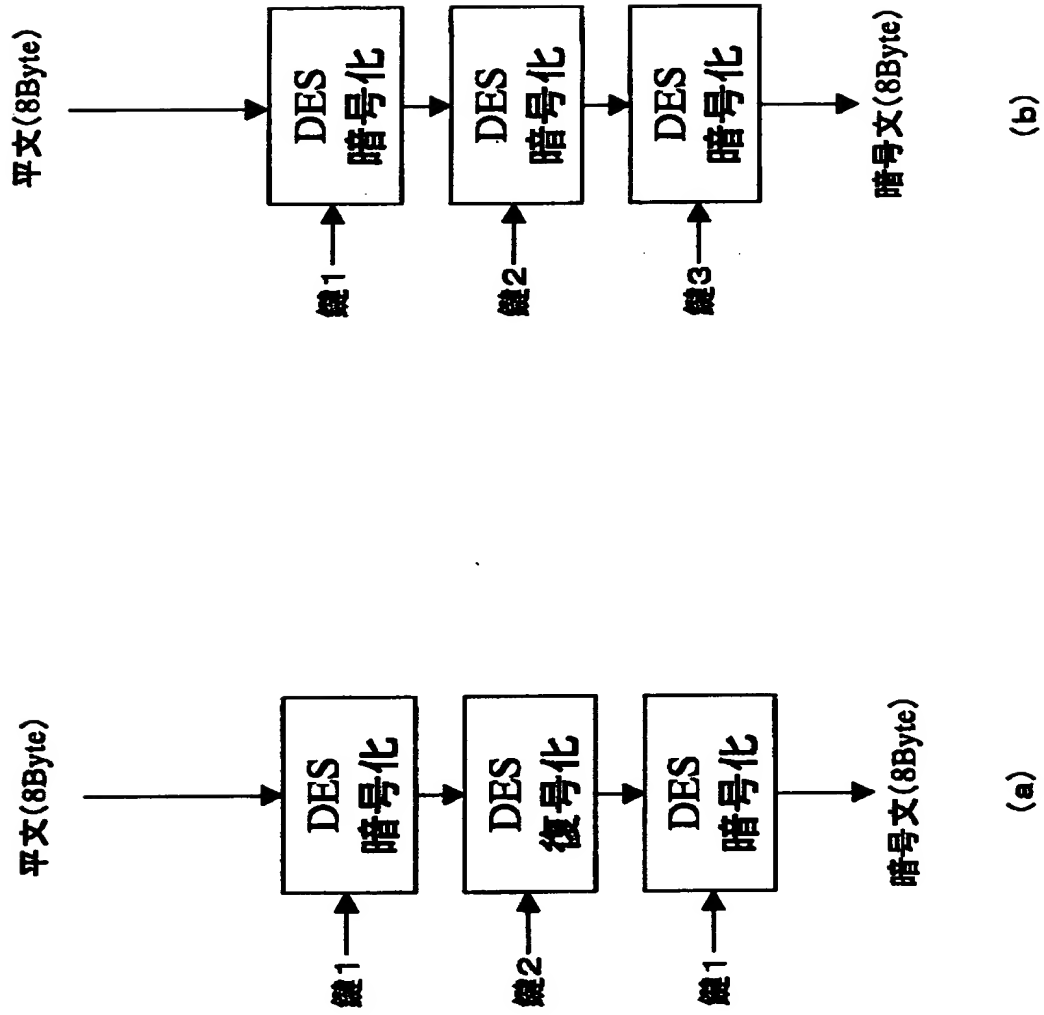
【図 7】



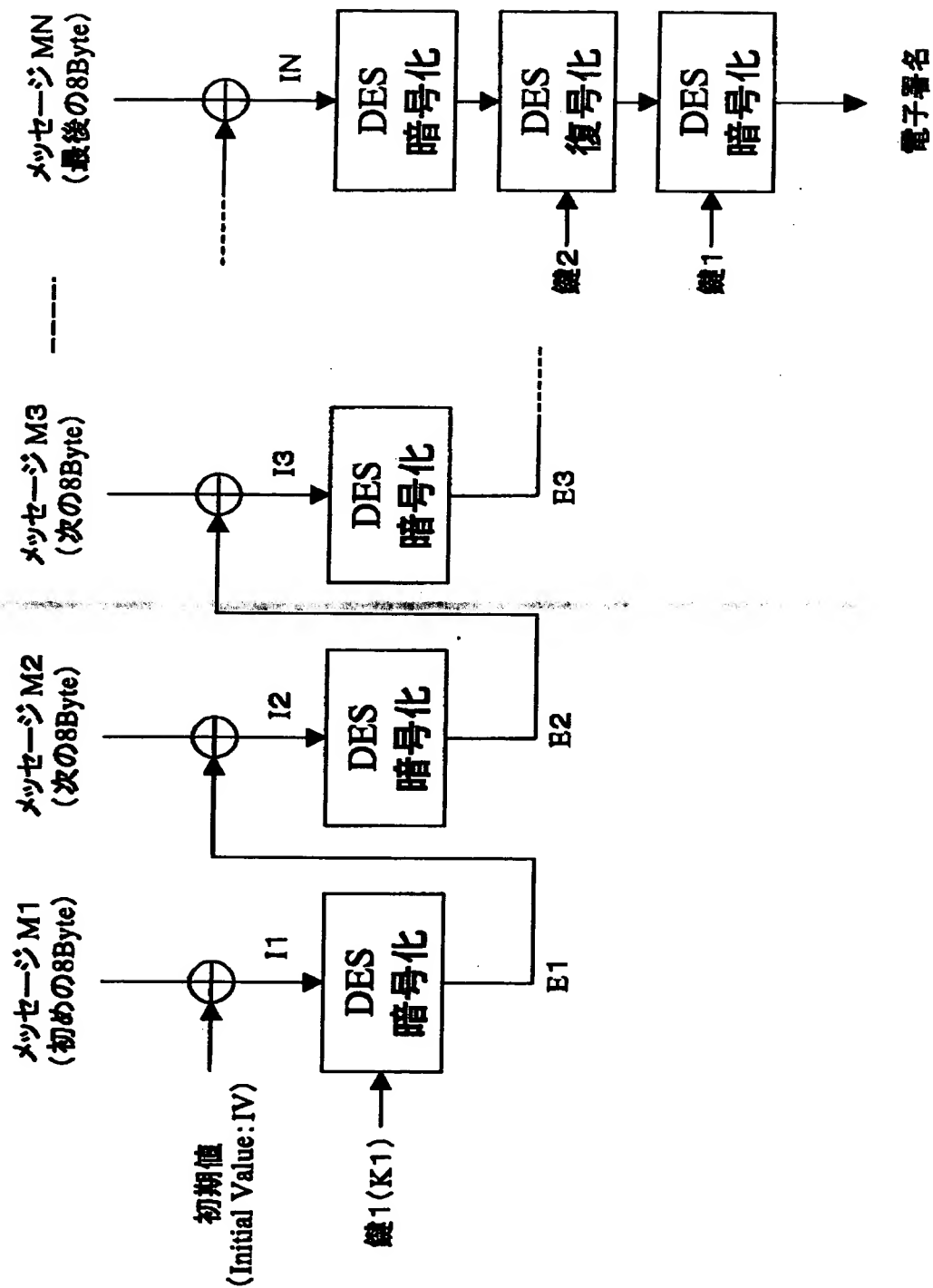
【図 8】



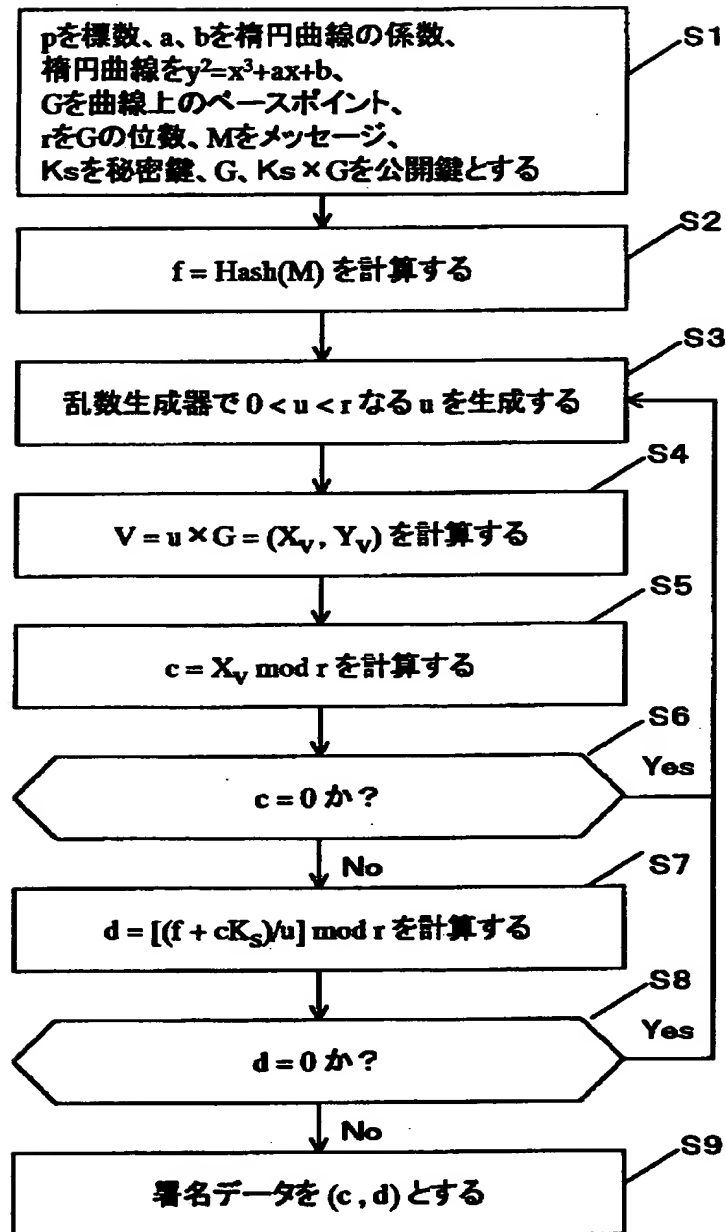
【図 9】



【図 10】

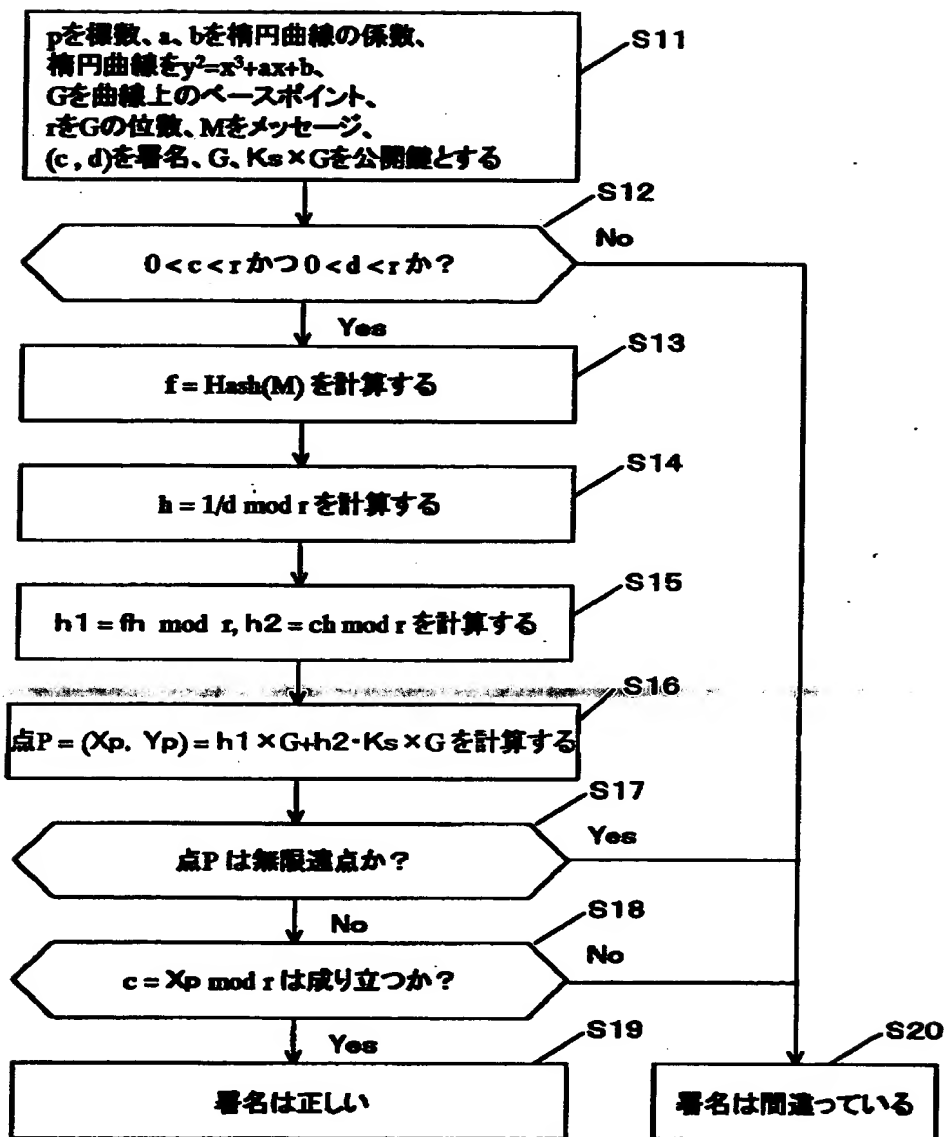


【図 11】

署名生成署名生成(IEEE P1363/D3)

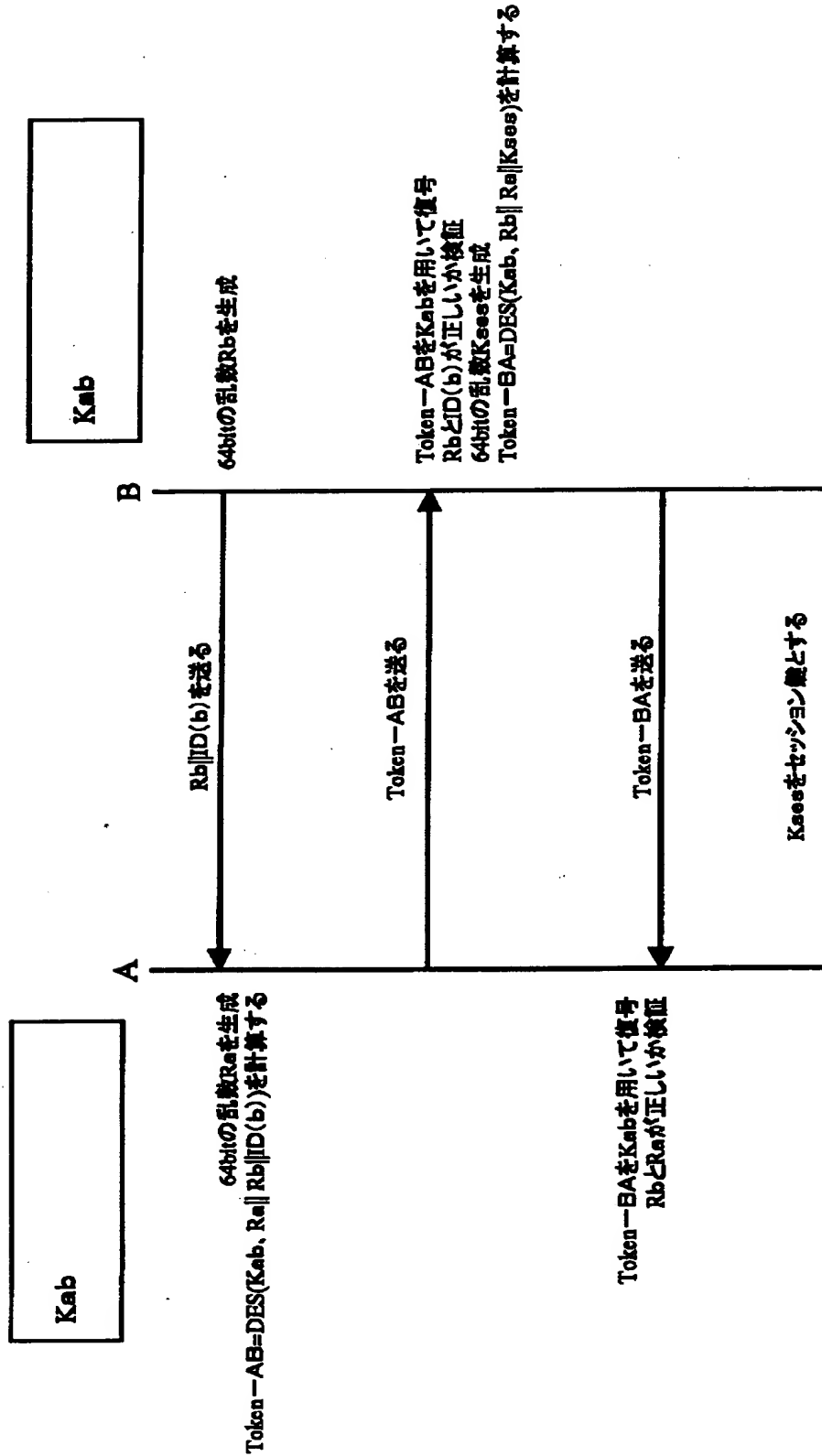
【図 12】

署名検証



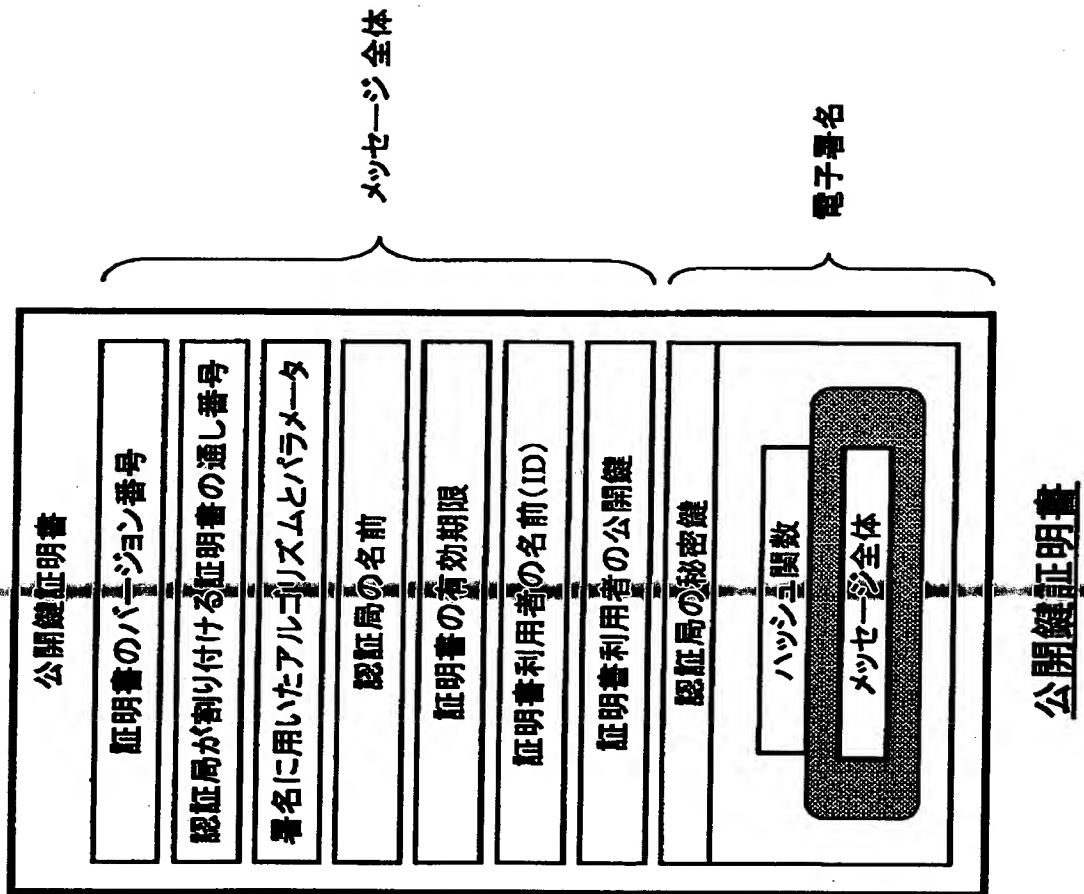
署名検証(IEEE P1363/D3)

【図 13】

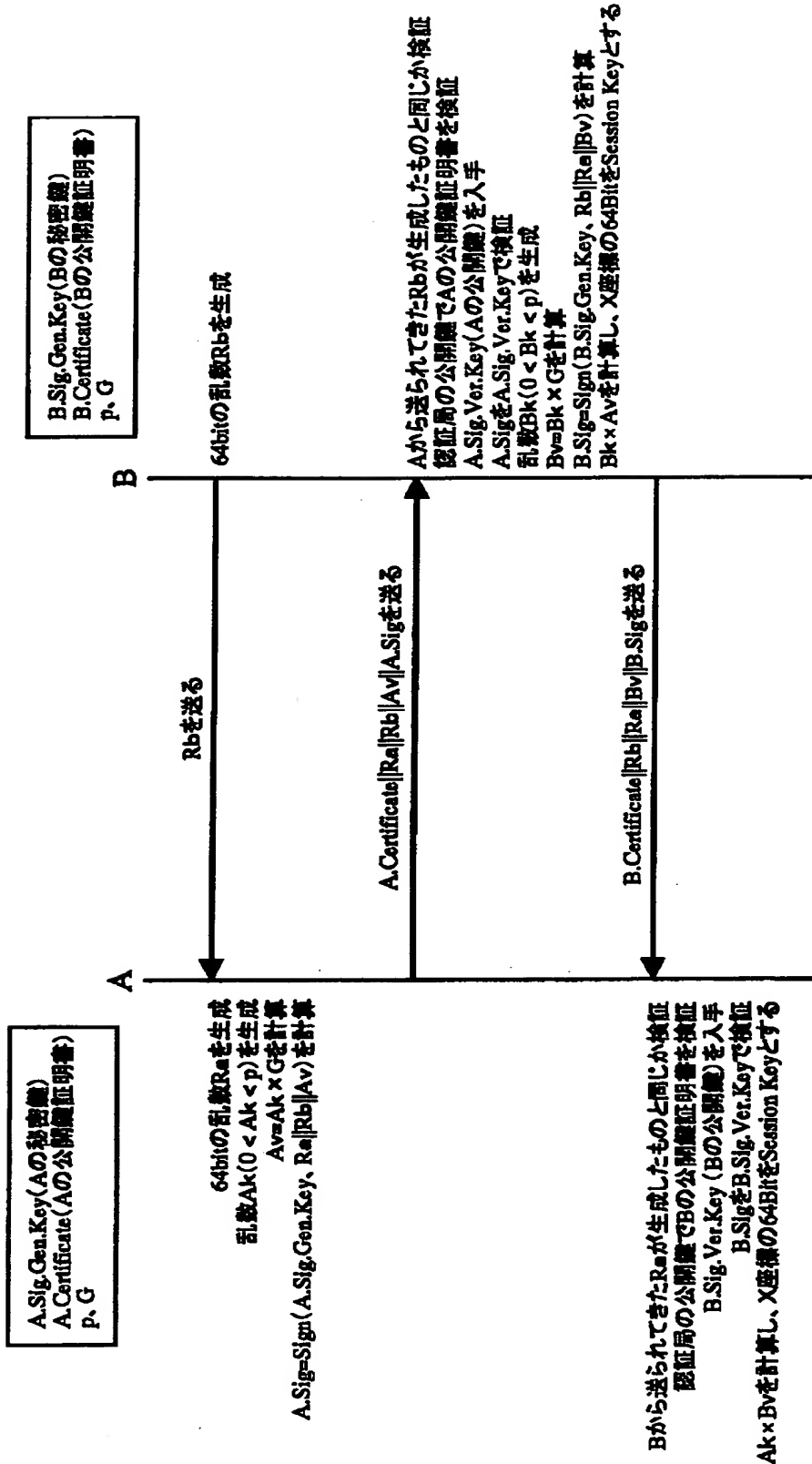


ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図14】

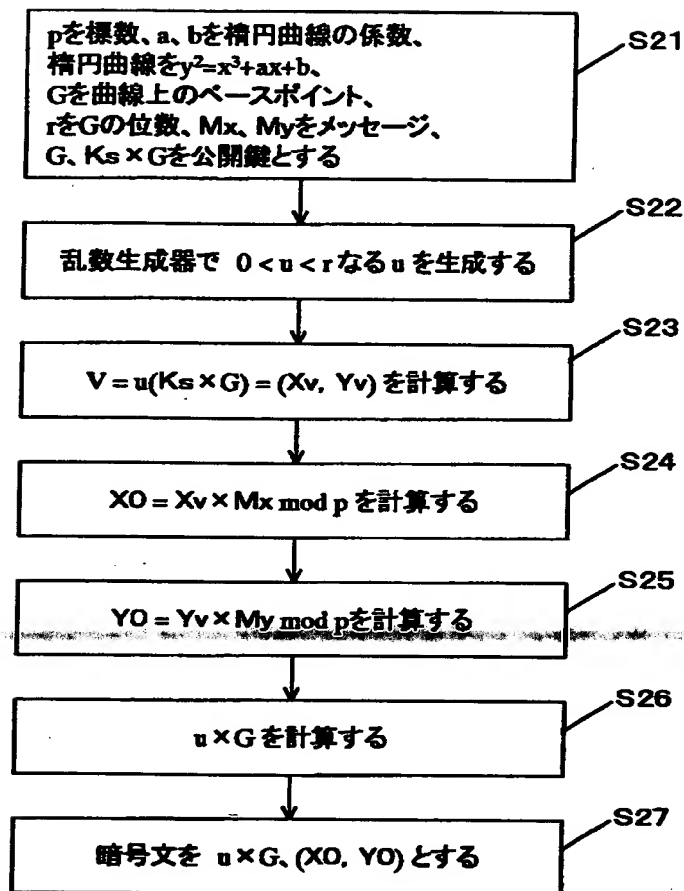


【図 1 5】

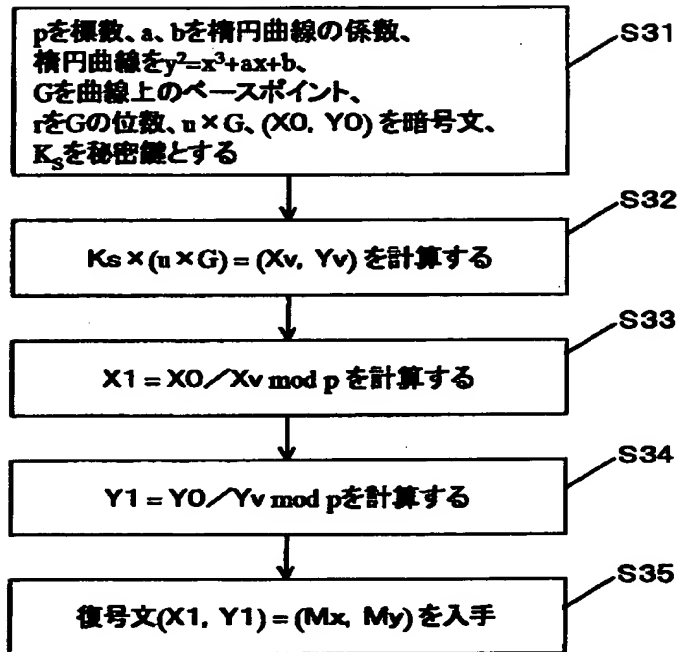


ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

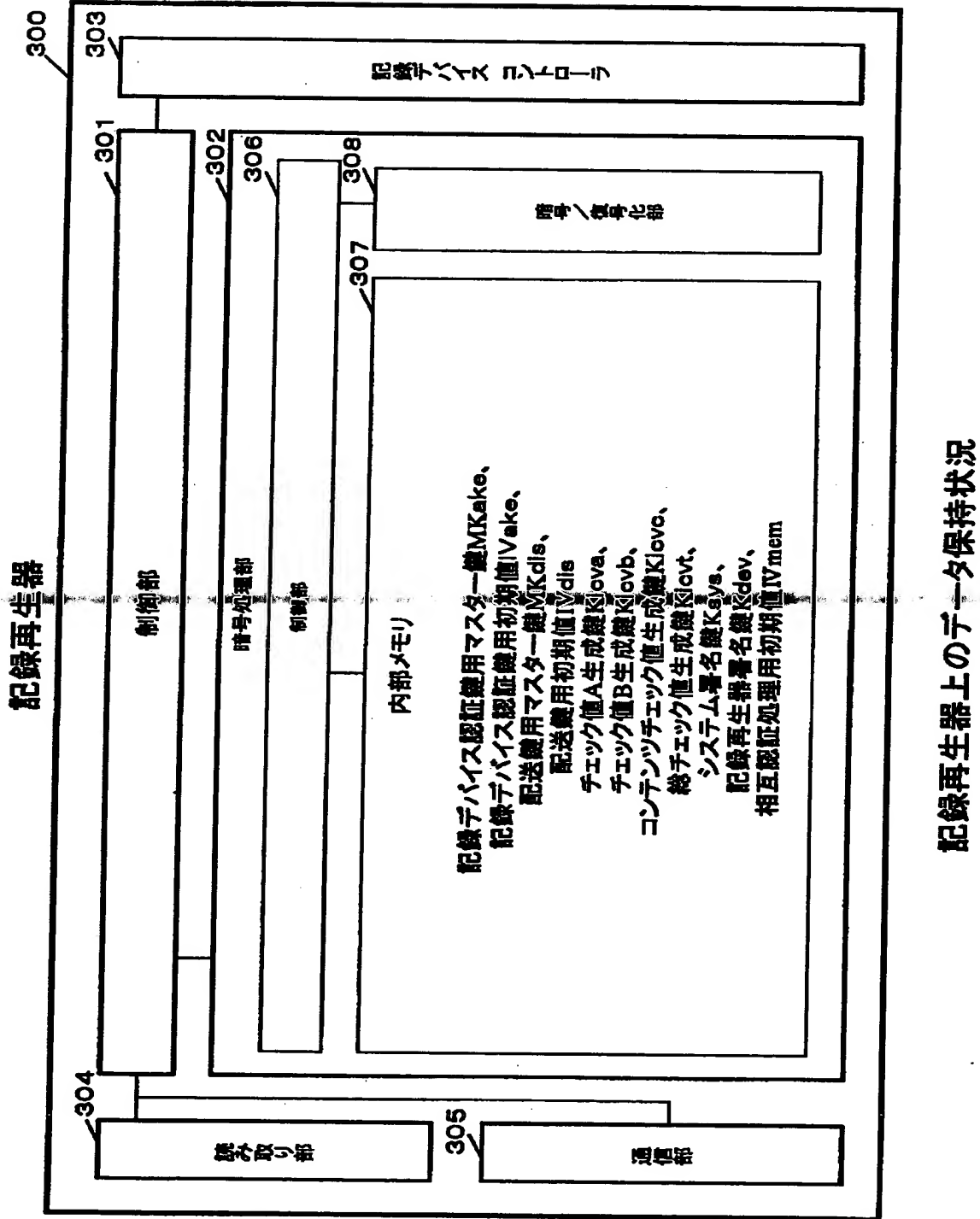
【図 1 6】

暗号化楕円曲線暗号を用いた暗号化(Menezes-Vanstone)

【図 17】

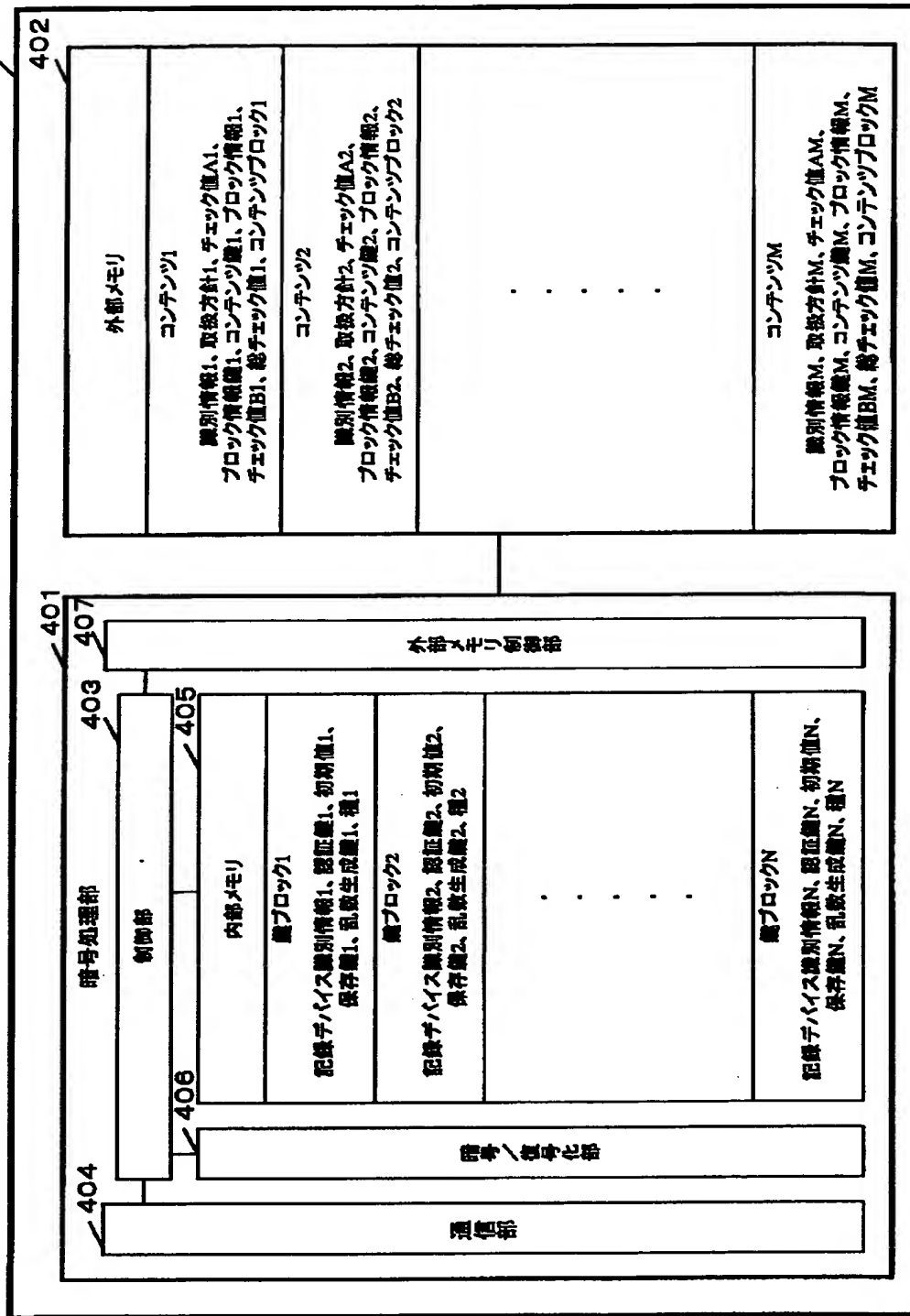
復号化楕円曲線暗号を用いた復号化(Menezes-Vanstone)

【図 18】



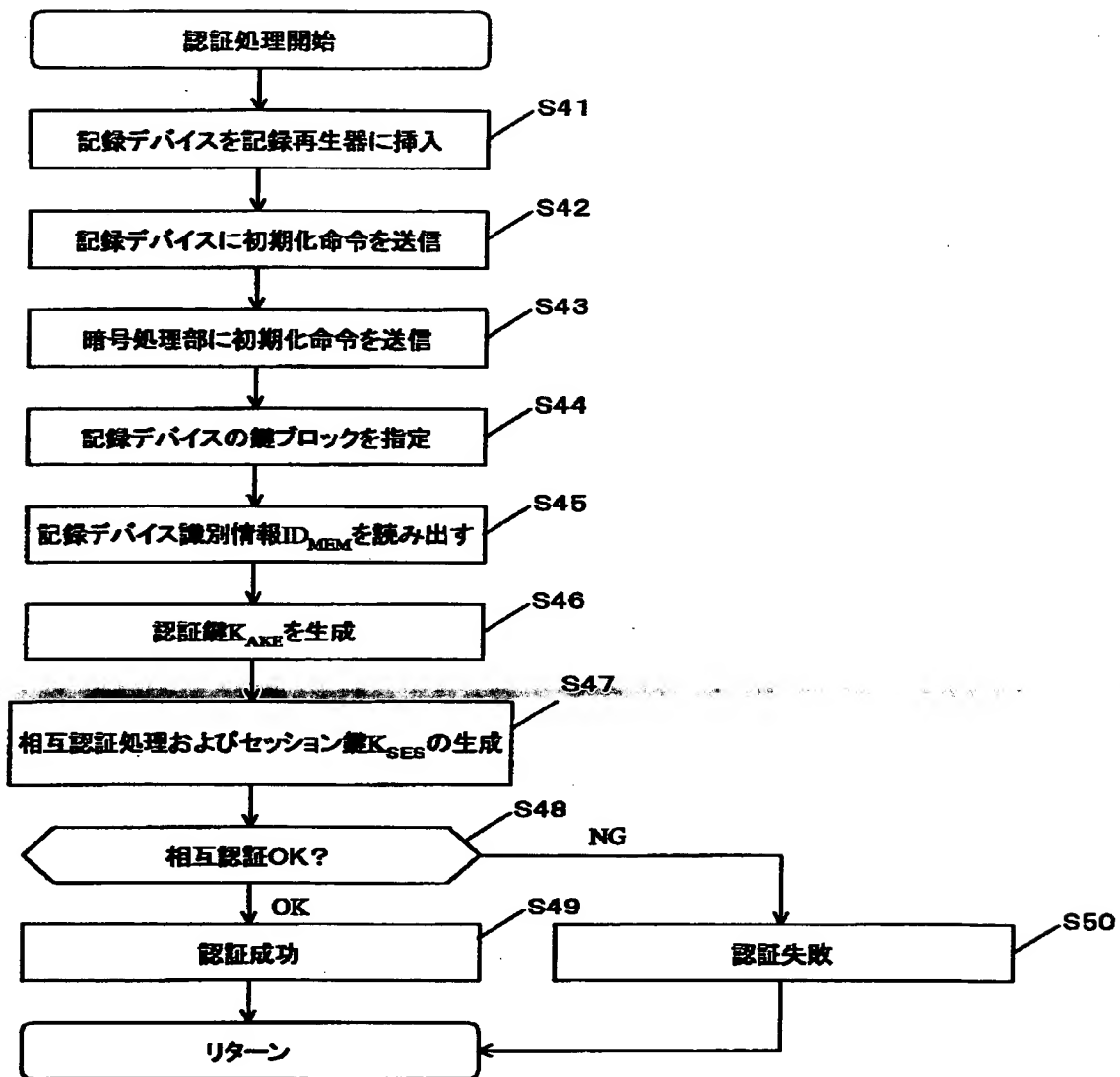
【図 19】

記録デバイス



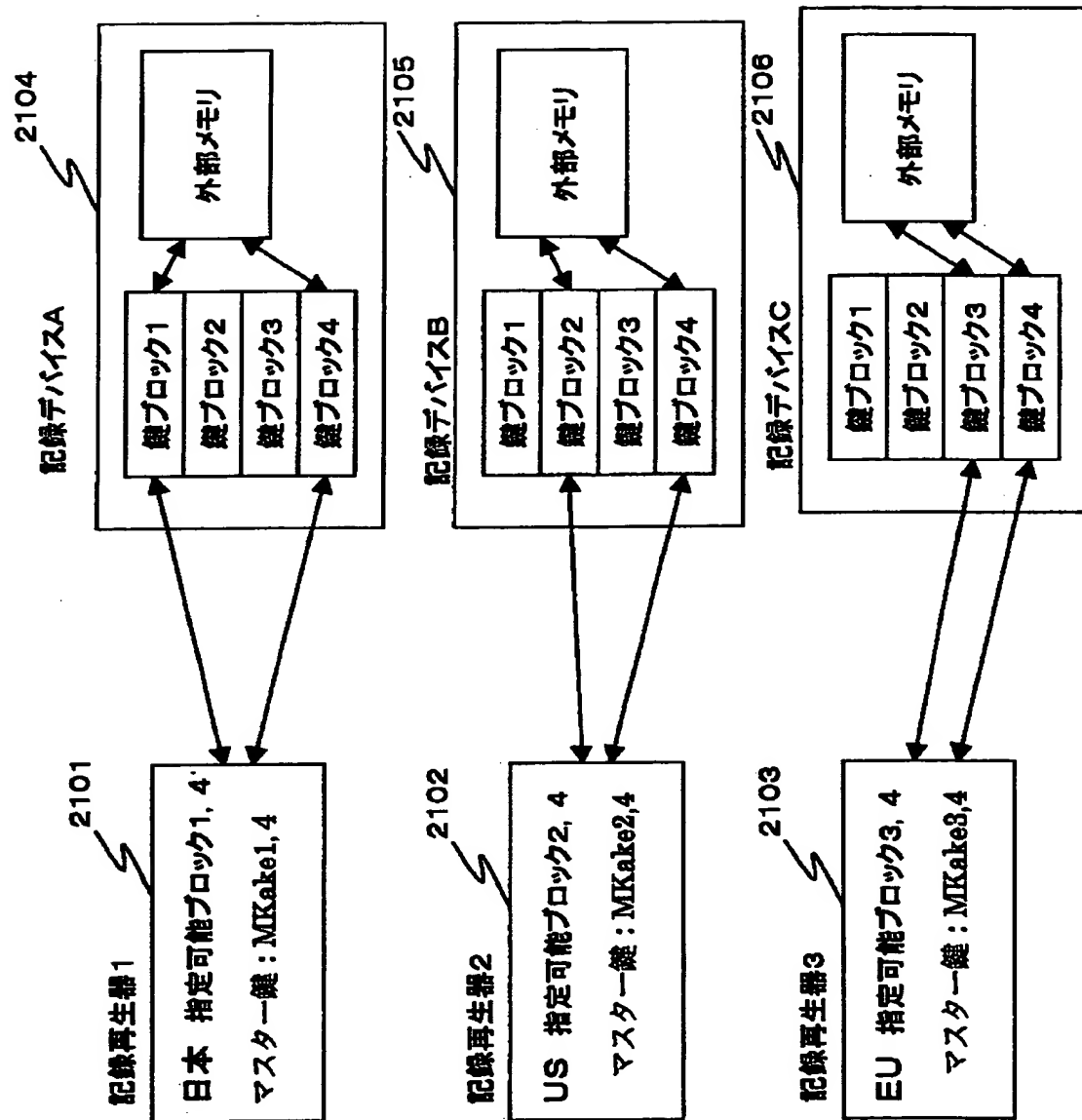
記録デバイス上のデータ保持状況

【図 20】

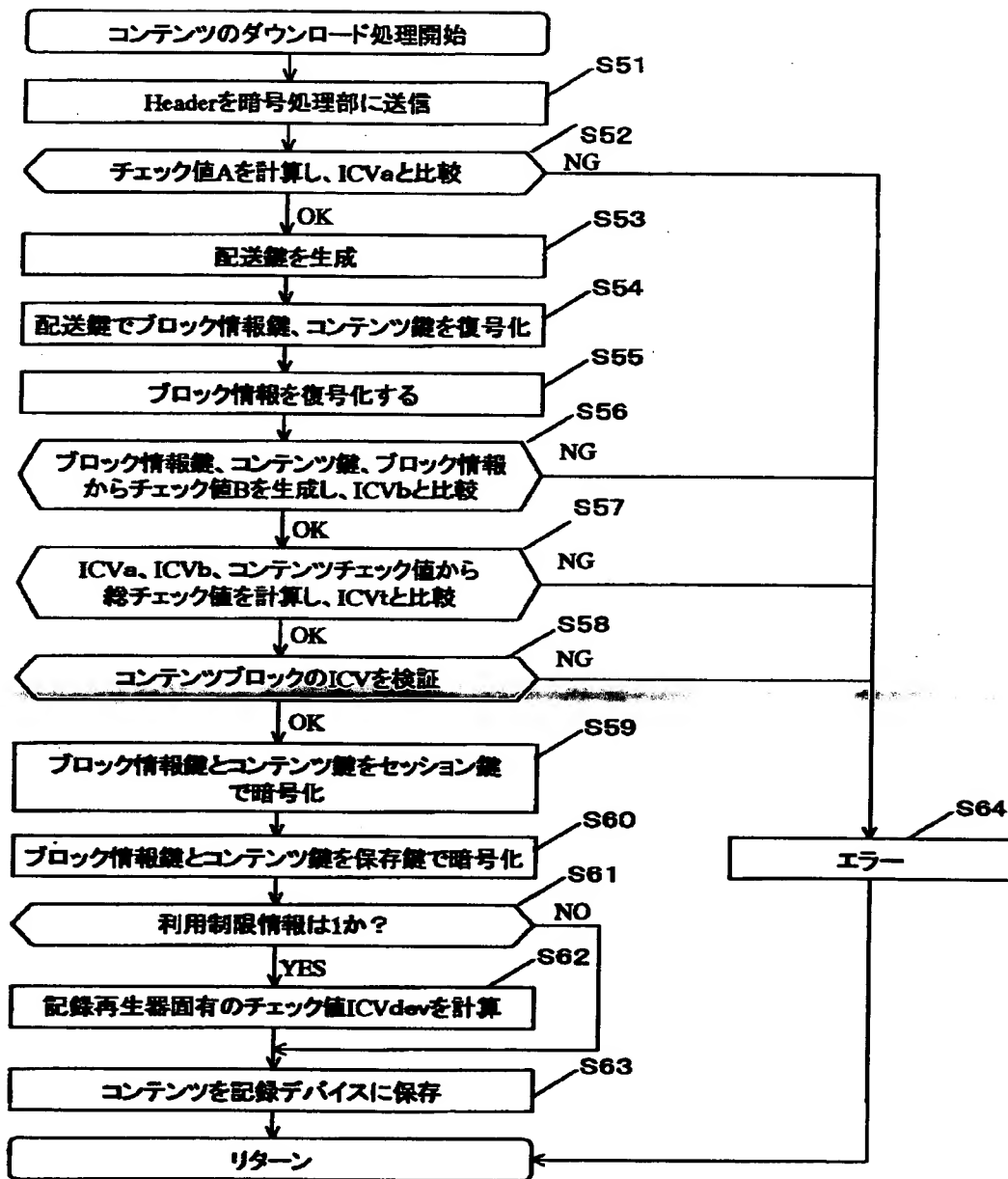


記録再生器と記録デバイスとの相互認証

【図 21】

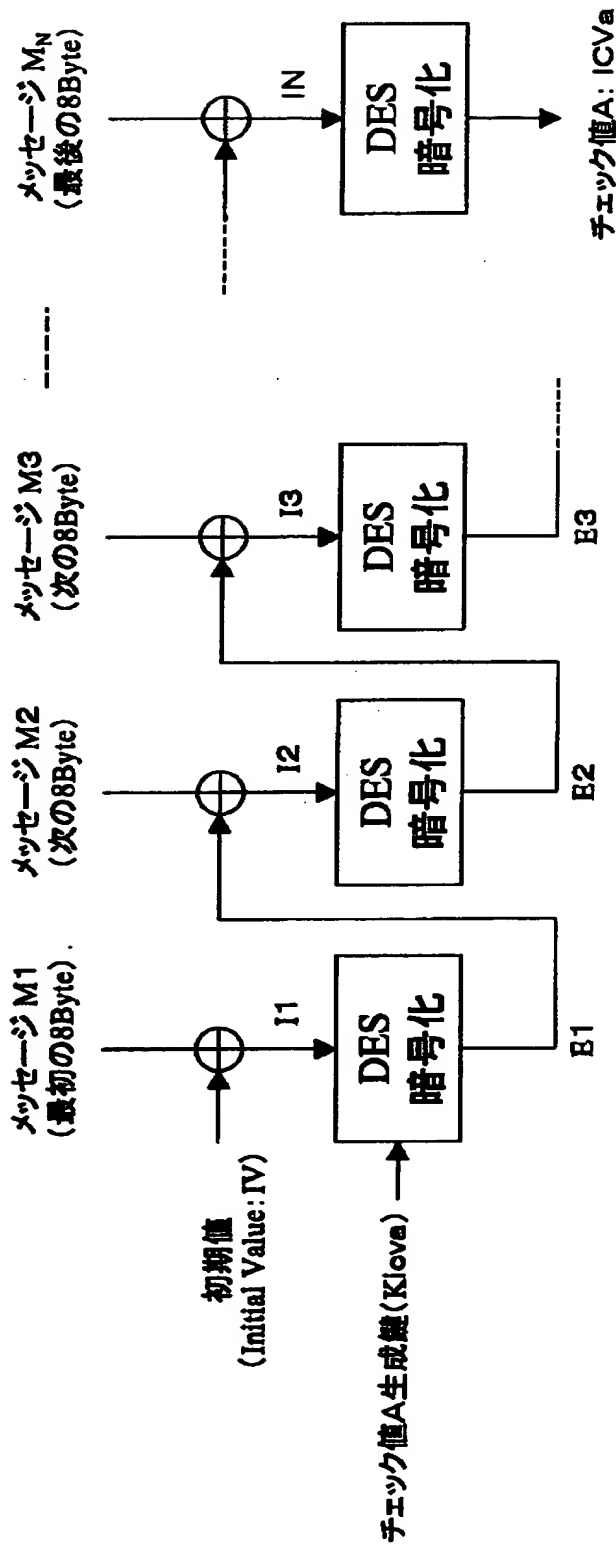


【図 2 2】



コンテンツのダウンロード処理

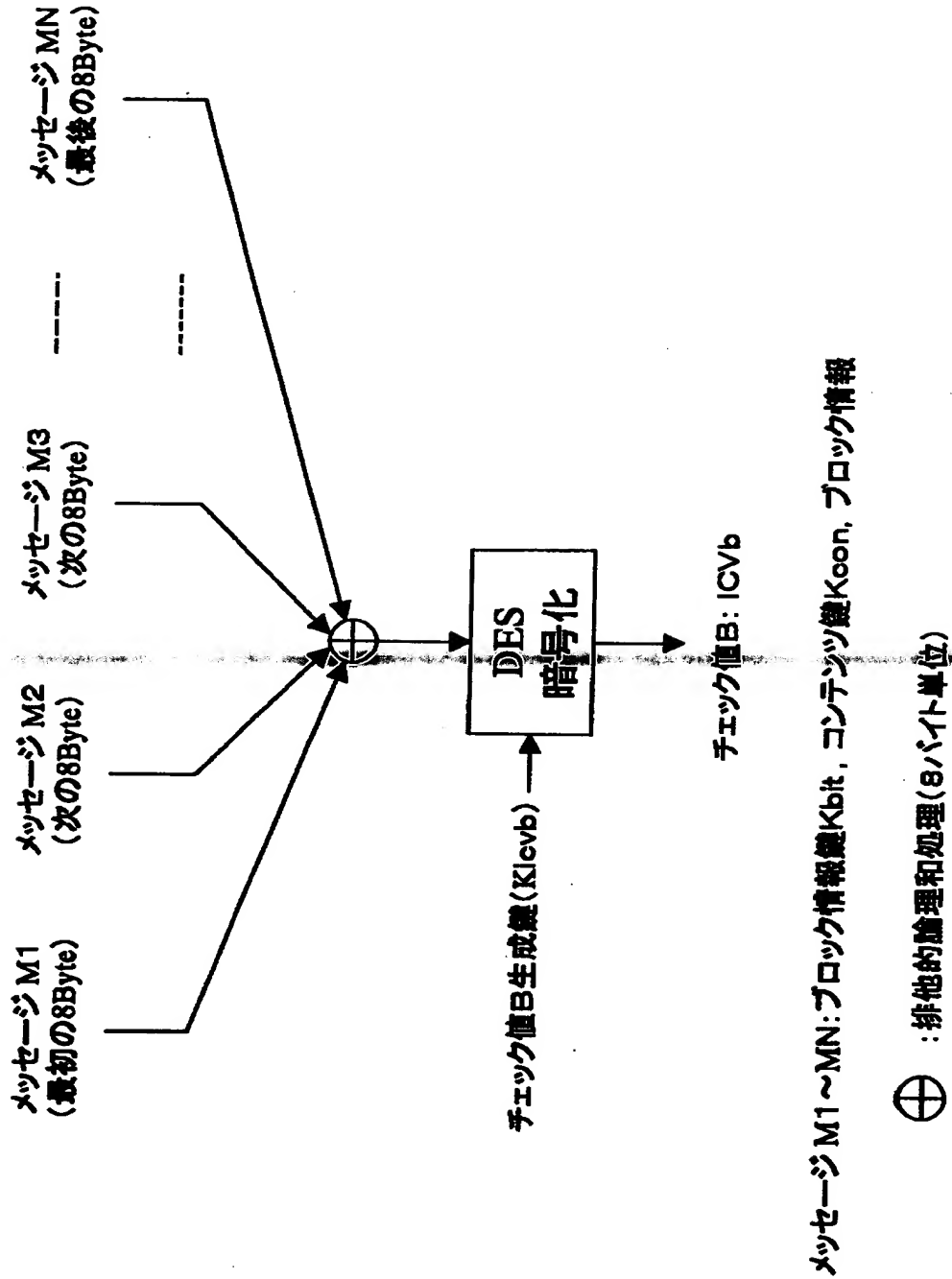
【図 23】



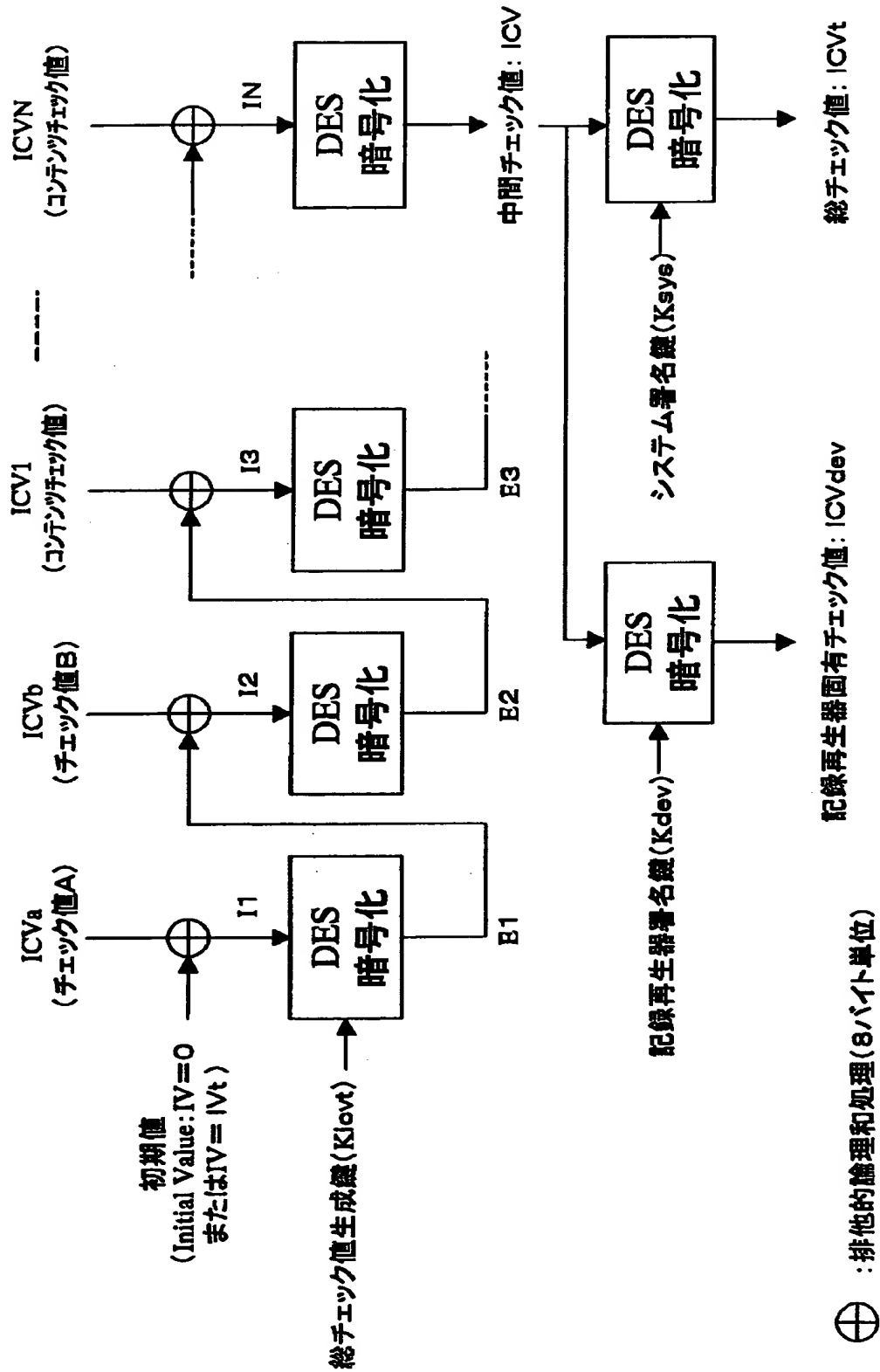
メッセージ M1 ~ MN: 識別情報, 取扱方針

⊕: 排他的論理和処理(8バイト単位)

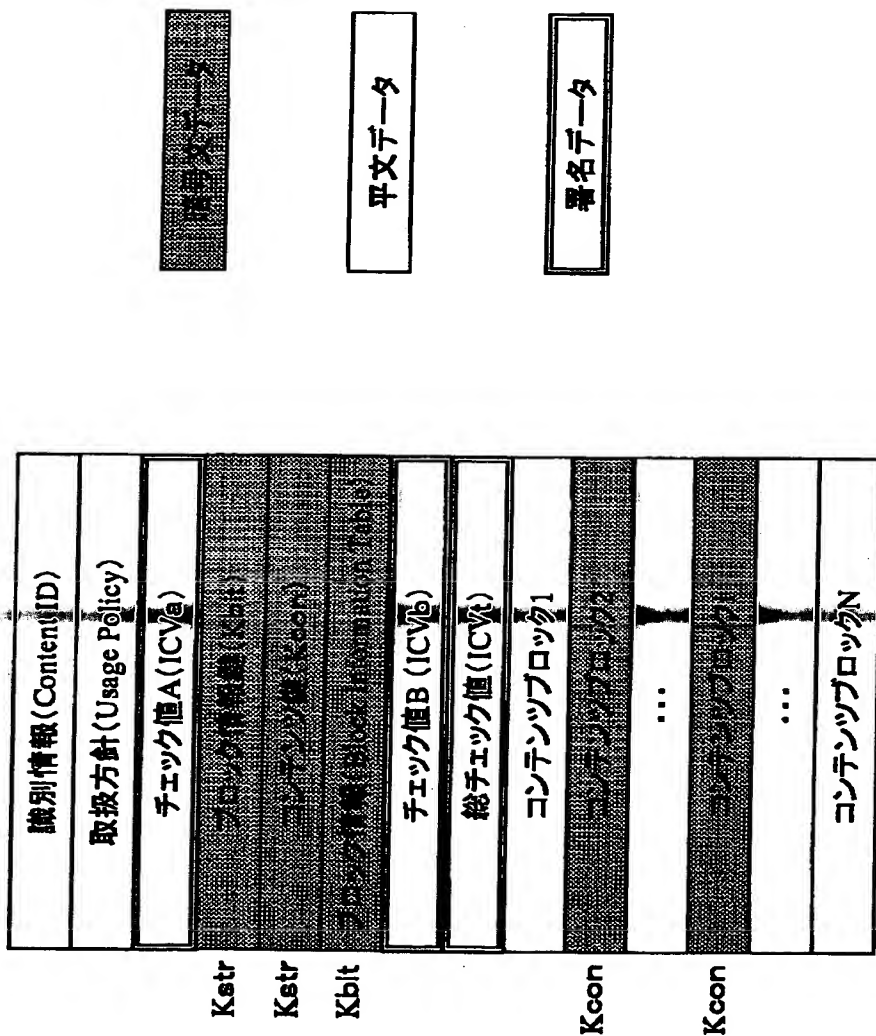
【図 24】



【図 25】

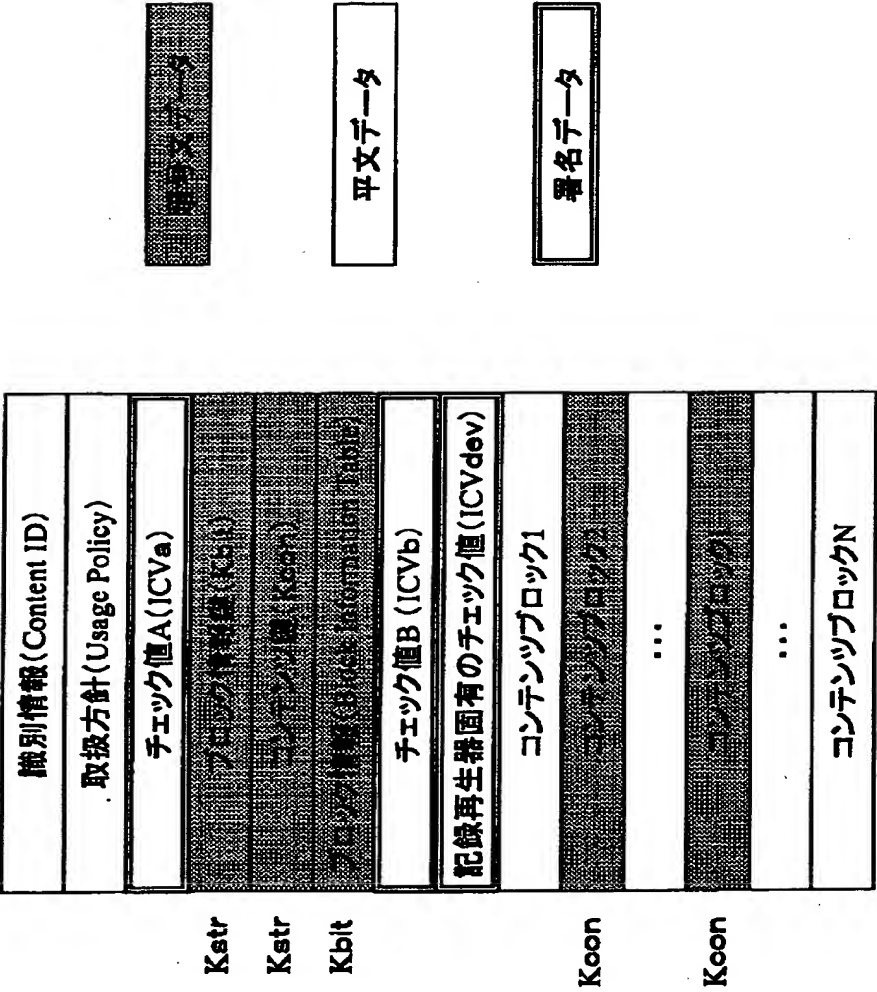


【図 2 6】



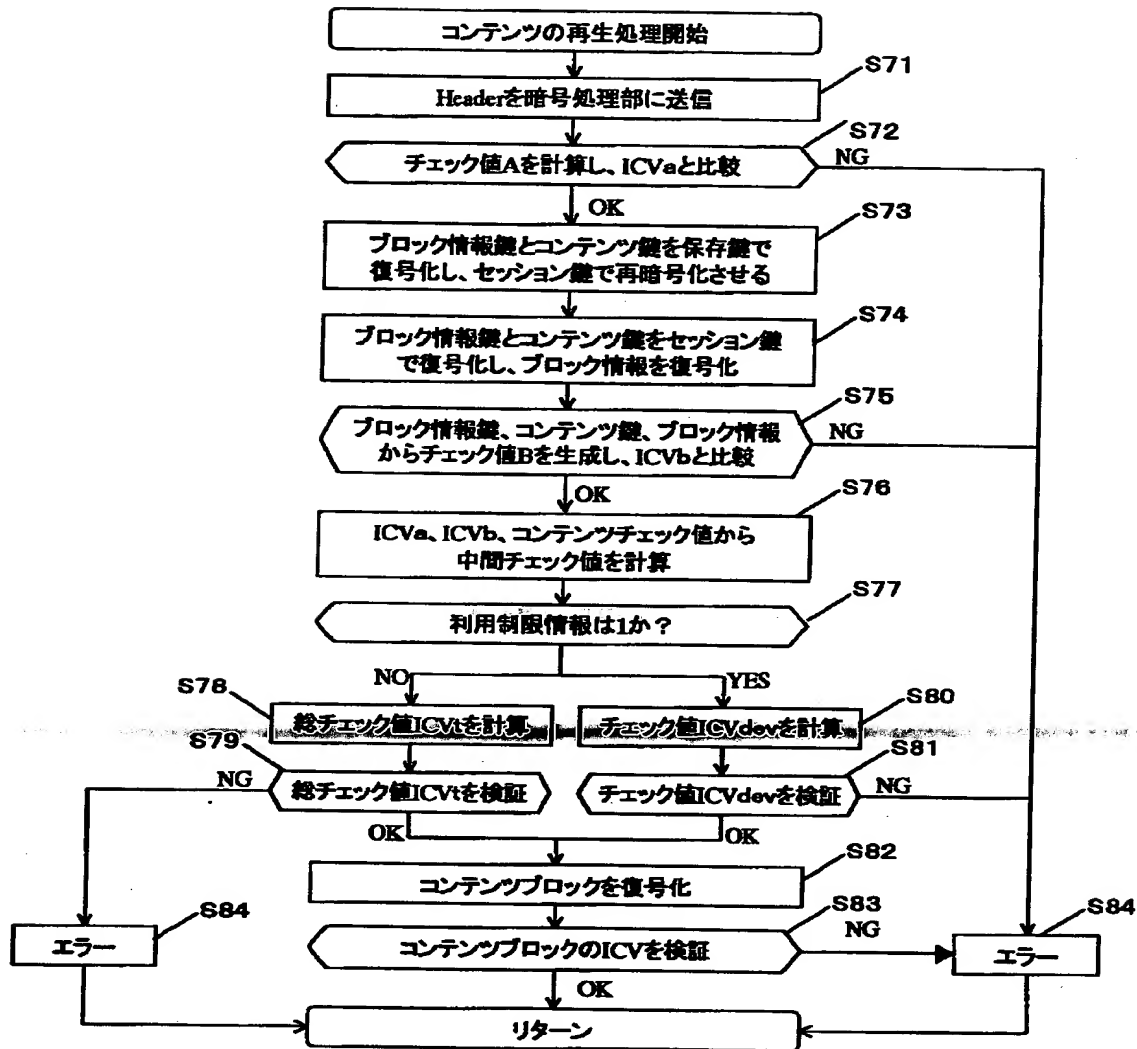
記録デバイスに保存されたコンテンツ
(利用制限情報=0)

【図 2 7】



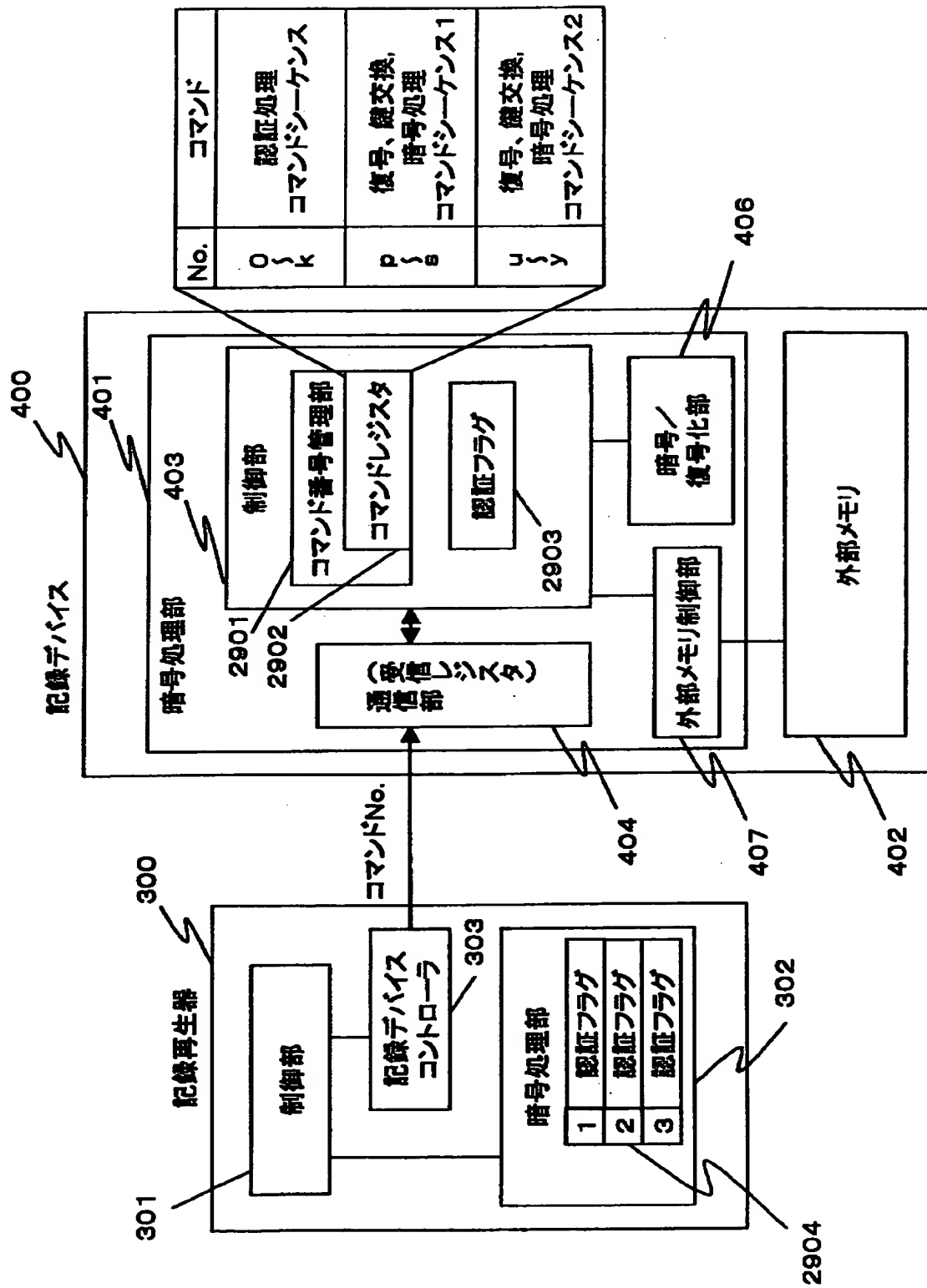
記録デバイスに保存されたコンテンツ
(利用制限情報=1)

【図 28】

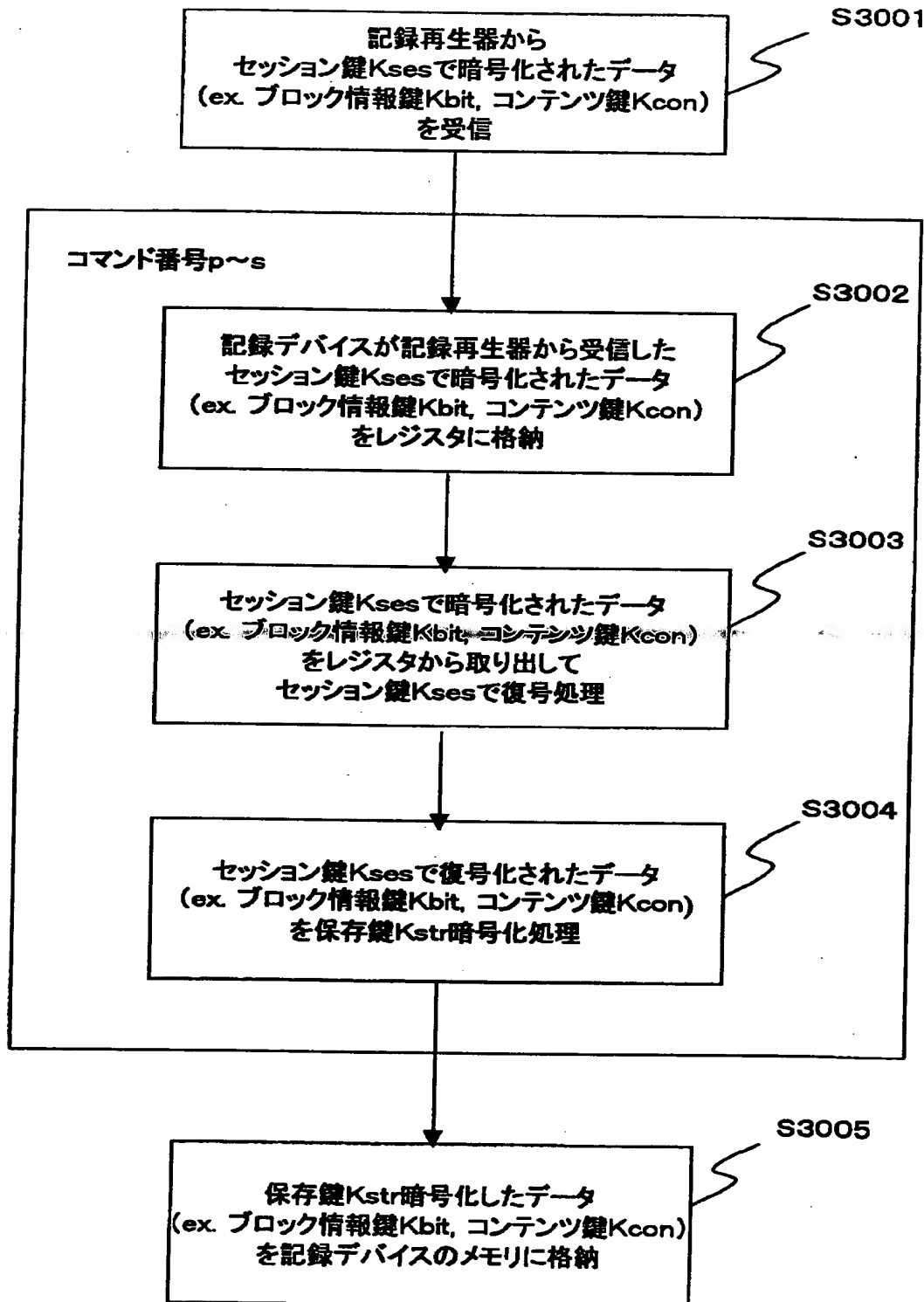


コンテンツの再生処理

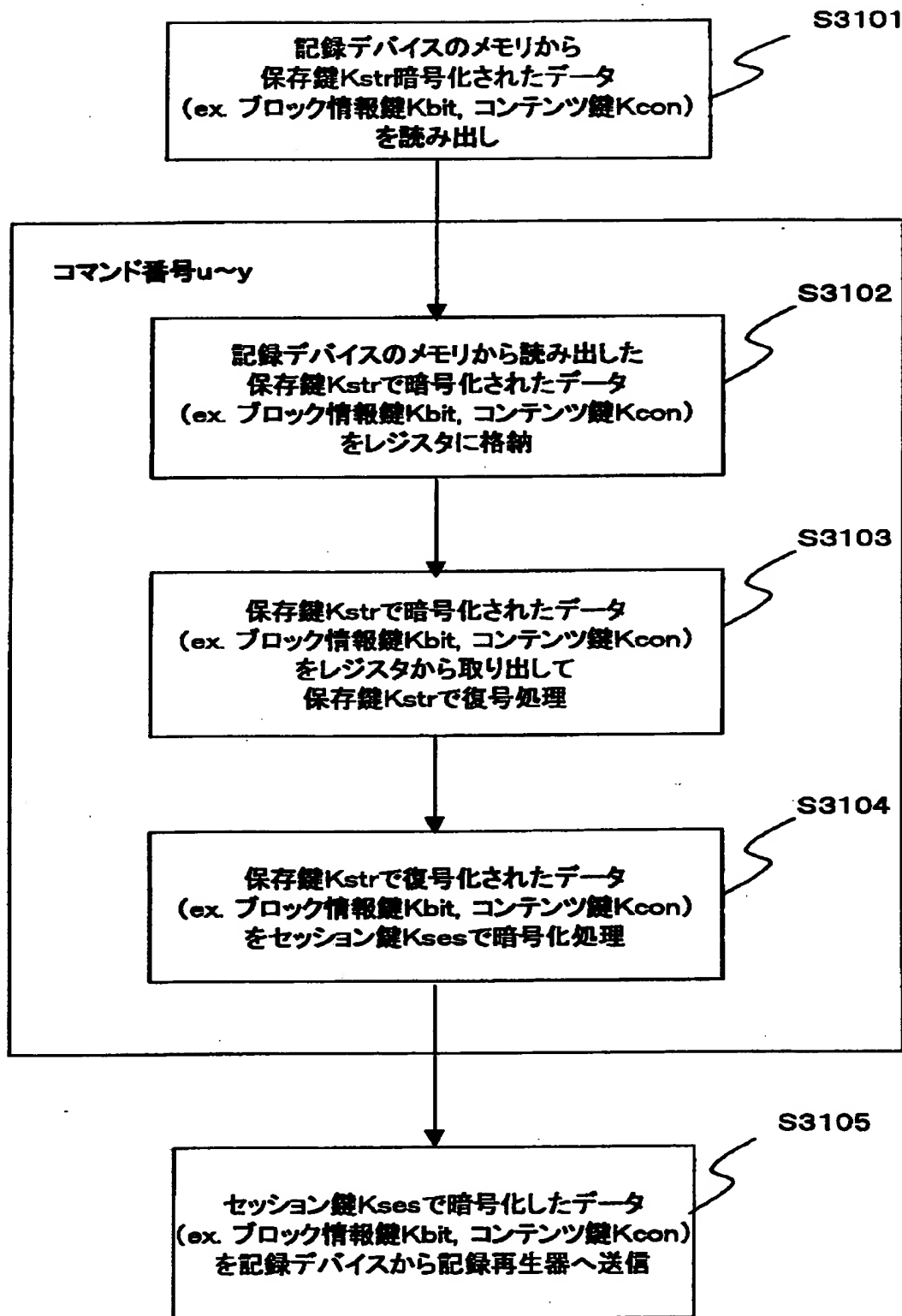
【図 29】



【図 30】



【図 31】



【図32】

フォーマット・タイプ0

| | |
|------|----------------------------------|
| | 識別情報 (Content ID) |
| | 取扱方針 (Usage Policy) |
| | チェック値A (ICV _a) |
| Kdis | ブロック情報 (Block Information Table) |
| Kdis | コンテンツID (Kcatr) |
| Kbit | ブロック情報 (Block Information Table) |
| | チェック値B (ICV _b) |
| | 総チェック値 (ICV _t) |
| | コンテンツブロック1 |
| Koon | コンテンツブロック2 |
| | ... |
| Koon | コンテンツブロックN |
| | コンテンツブロックN |

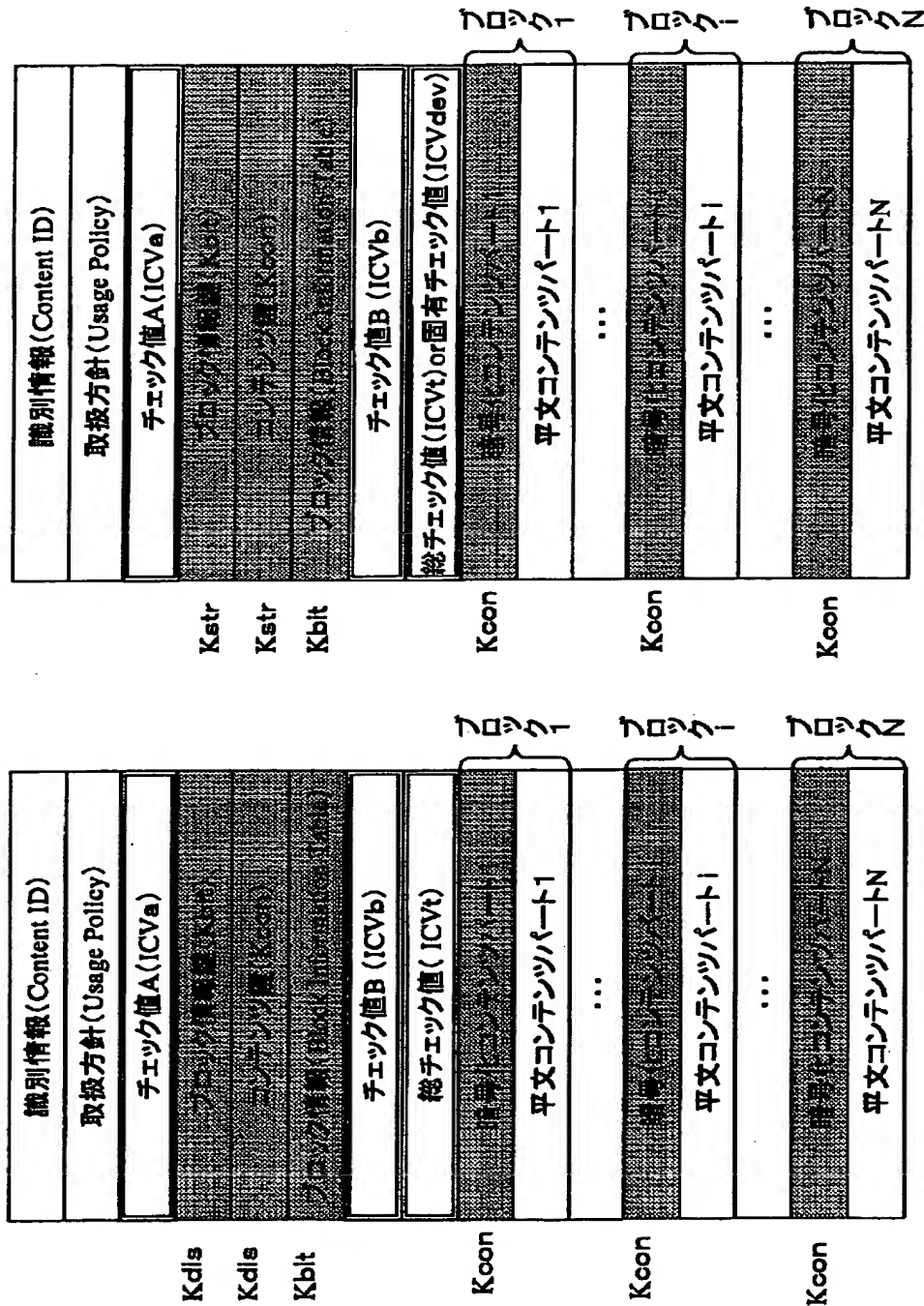
| | |
|------|---|
| | 識別情報 (Content ID) |
| | 取扱方針 (Usage Policy) |
| | チェック値A (ICV _a) |
| Katr | ブロック情報 (Block Information Table) |
| Katr | コンテンツID (Kcatr) |
| Kbit | ブロック情報 (Block Information Table) |
| | チェック値B (ICV _b) |
| | 総チェック値 (ICV _t) or 固有チェック値 (ICV _{dev}) |
| | コンテンツブロック1 |
| Koon | コンテンツブロック2 |
| | ... |
| Koon | コンテンツブロックN |
| | コンテンツブロックN |

メディア上及び通信路上のデータフォーマット 記録デバイスに保存されたコンテンツ

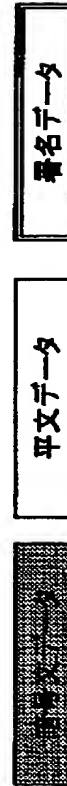
| | |
|--------|-------|
| 暗号文データ | 署名データ |
|--------|-------|

【図 33】

フォーマット・タイプ 1

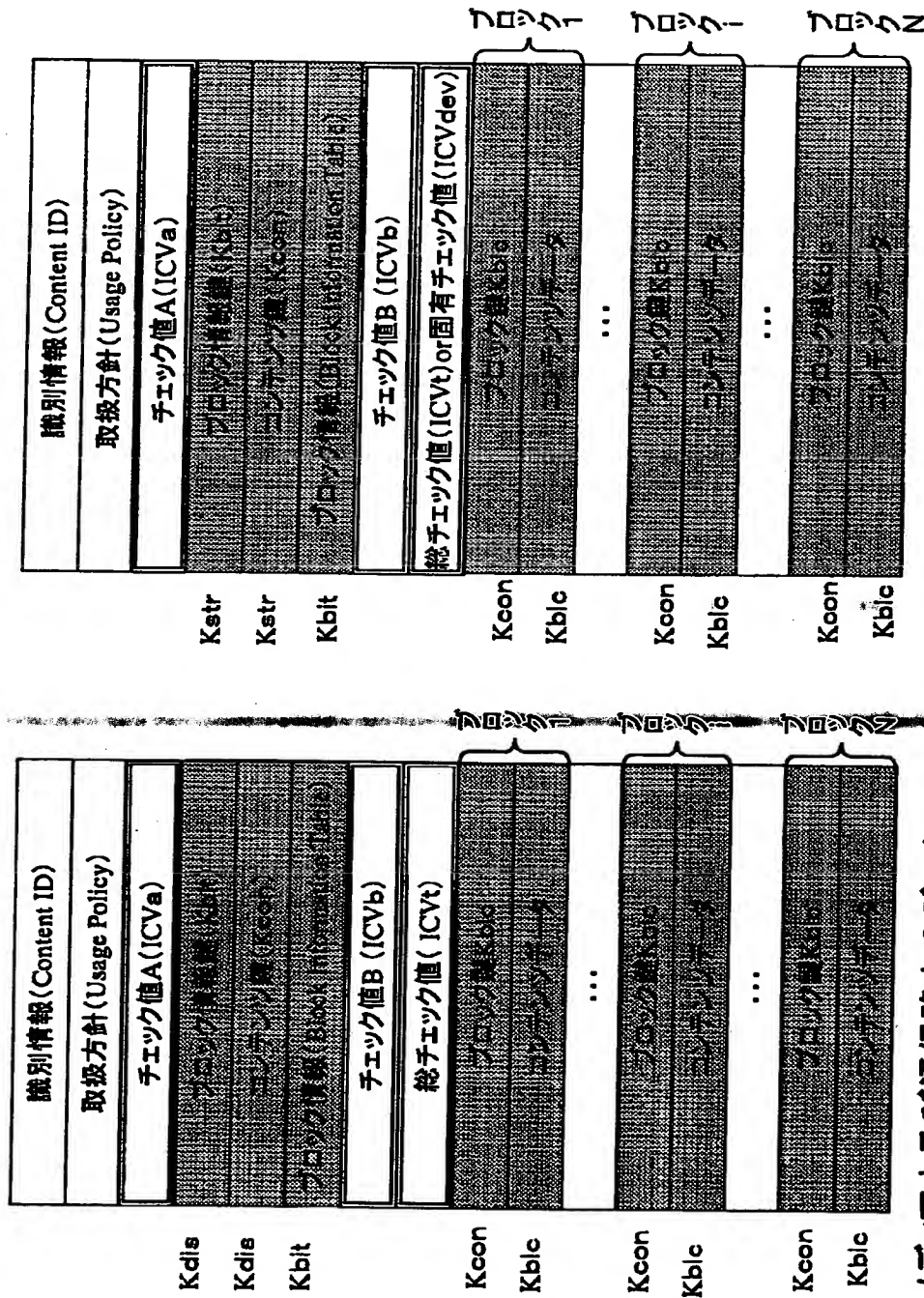


メディア上及び通信路上のデータフォーマット 記録デバイスに保存されたコンテンツ



【図 34】

フォーマット・タイプ 2

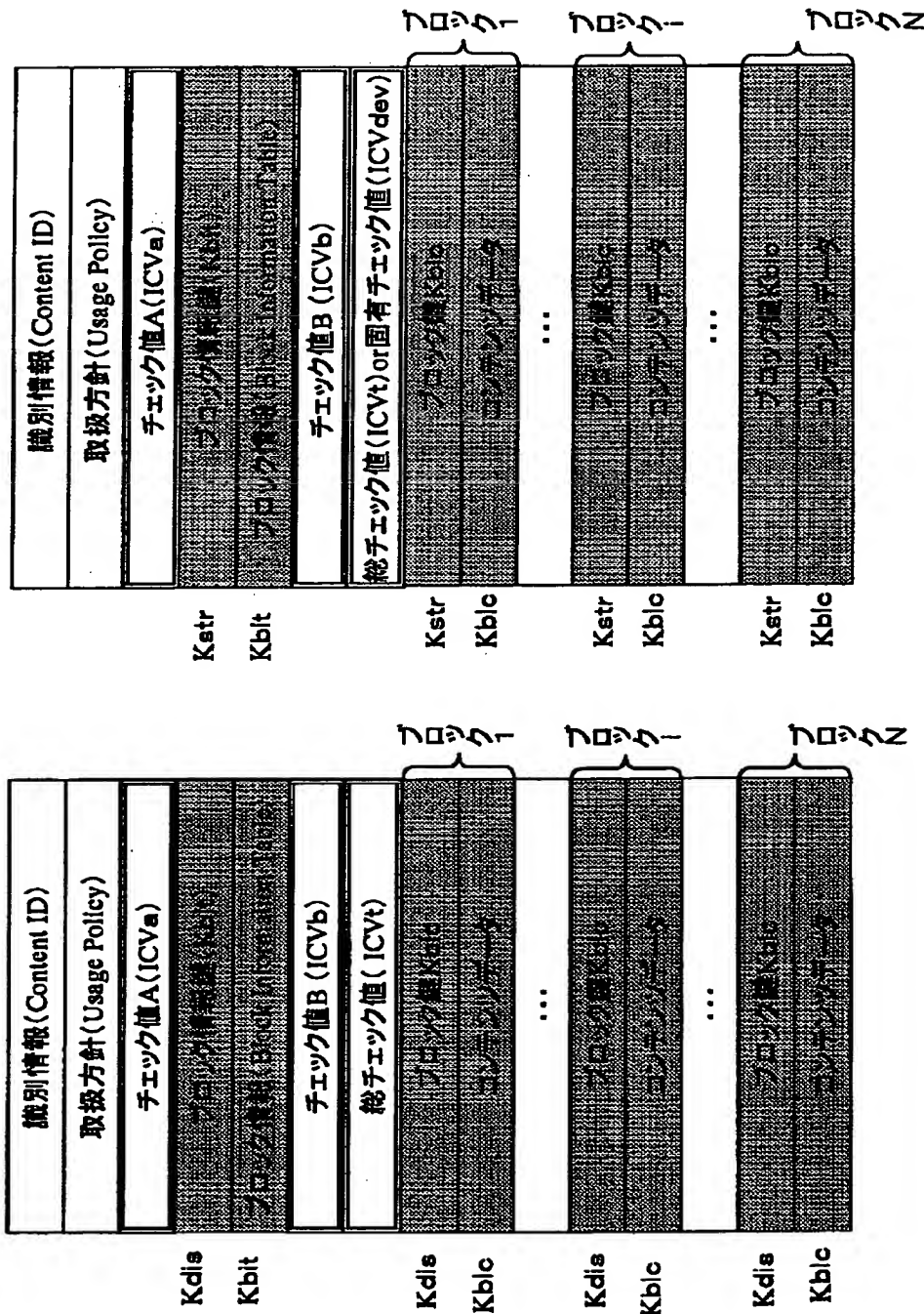


メディア上及び通信路上のデータフォーマット 記録デバイスに保存されたコンテンツ



【図 3 5】

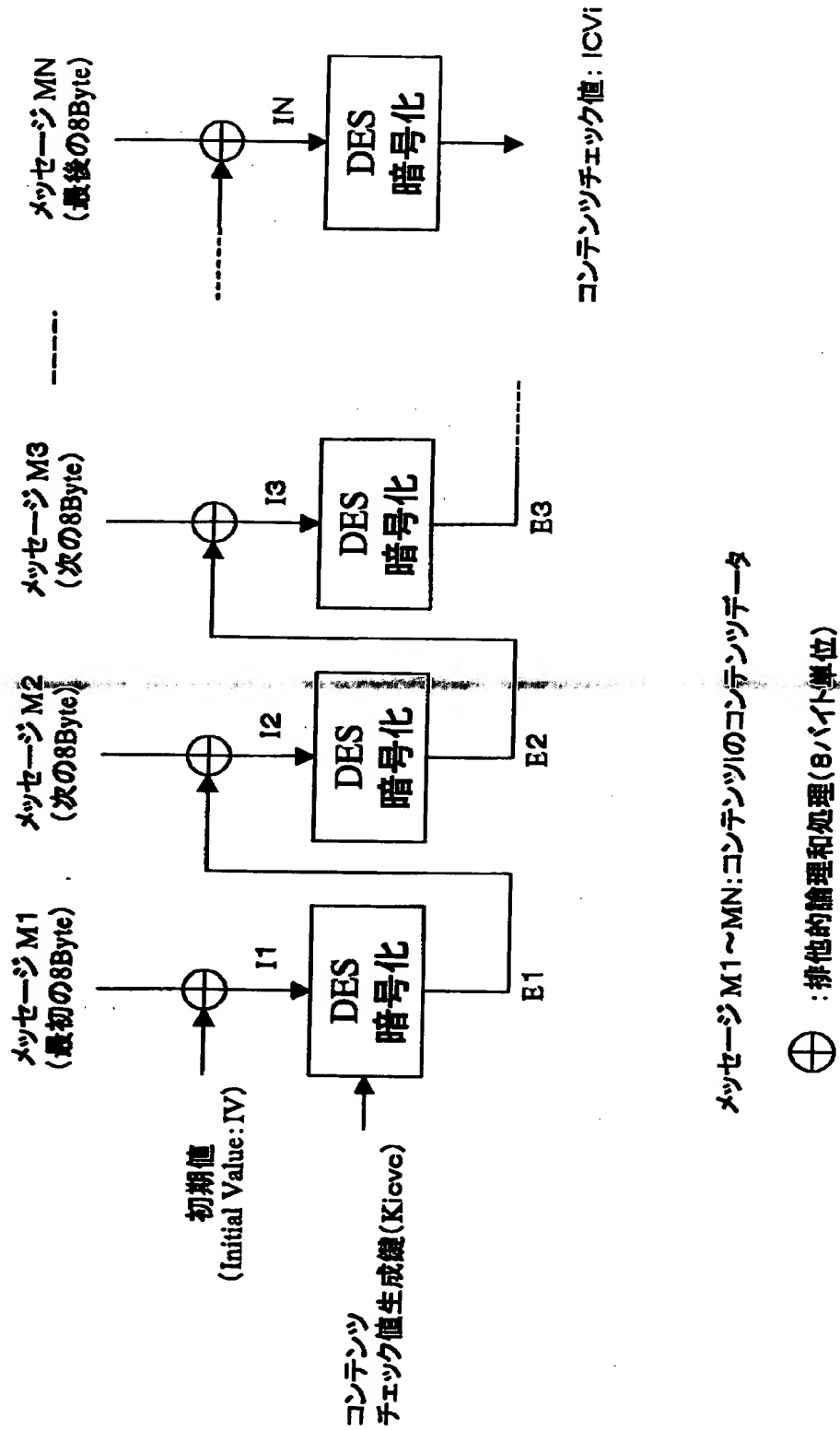
フォーマット・タイプ 3



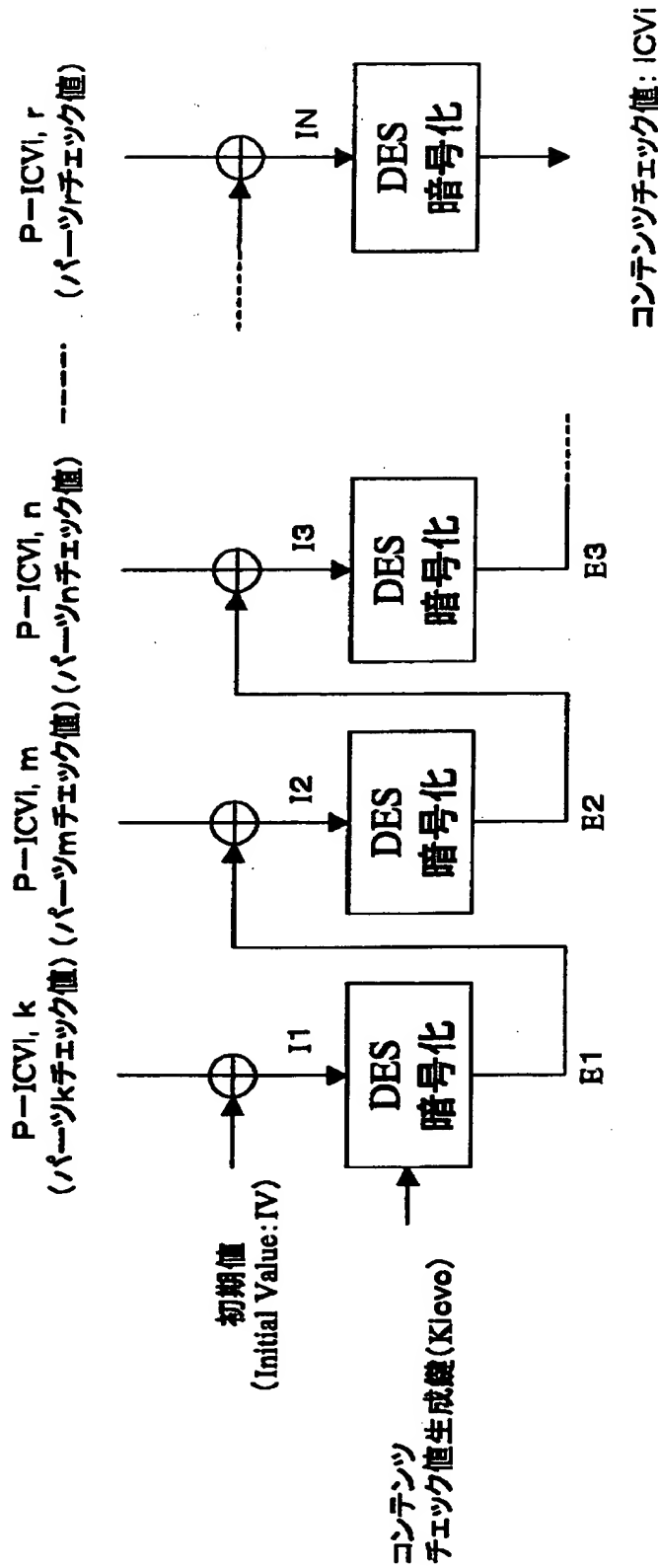
メディア上及び通信路上のデータフォーマット 記録デバイスに保存されたコンテンツ

| | | |
|-------|-------|-------|
| 暗号データ | 平文データ | 署名データ |
|-------|-------|-------|

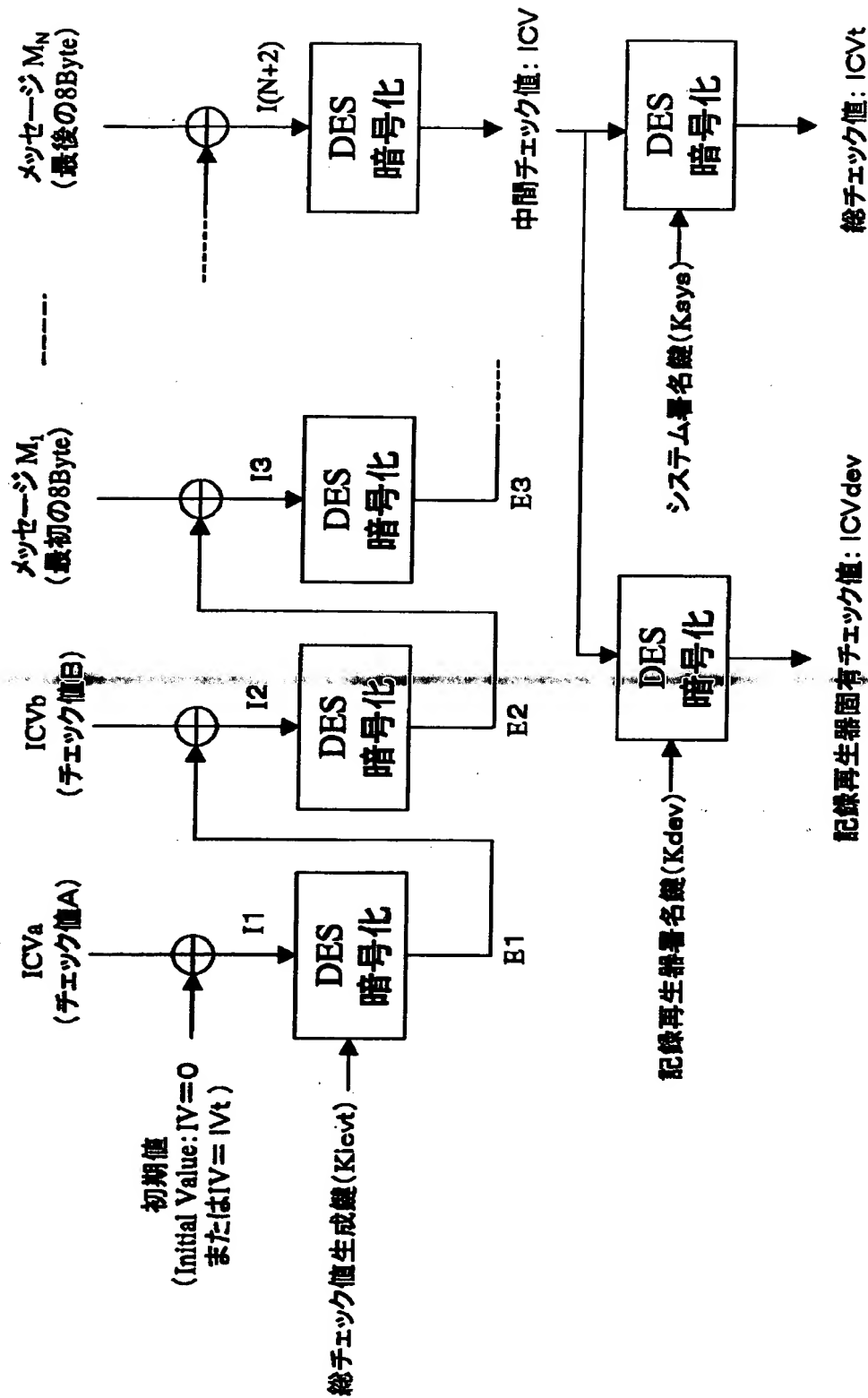
【図36】



【図 37】



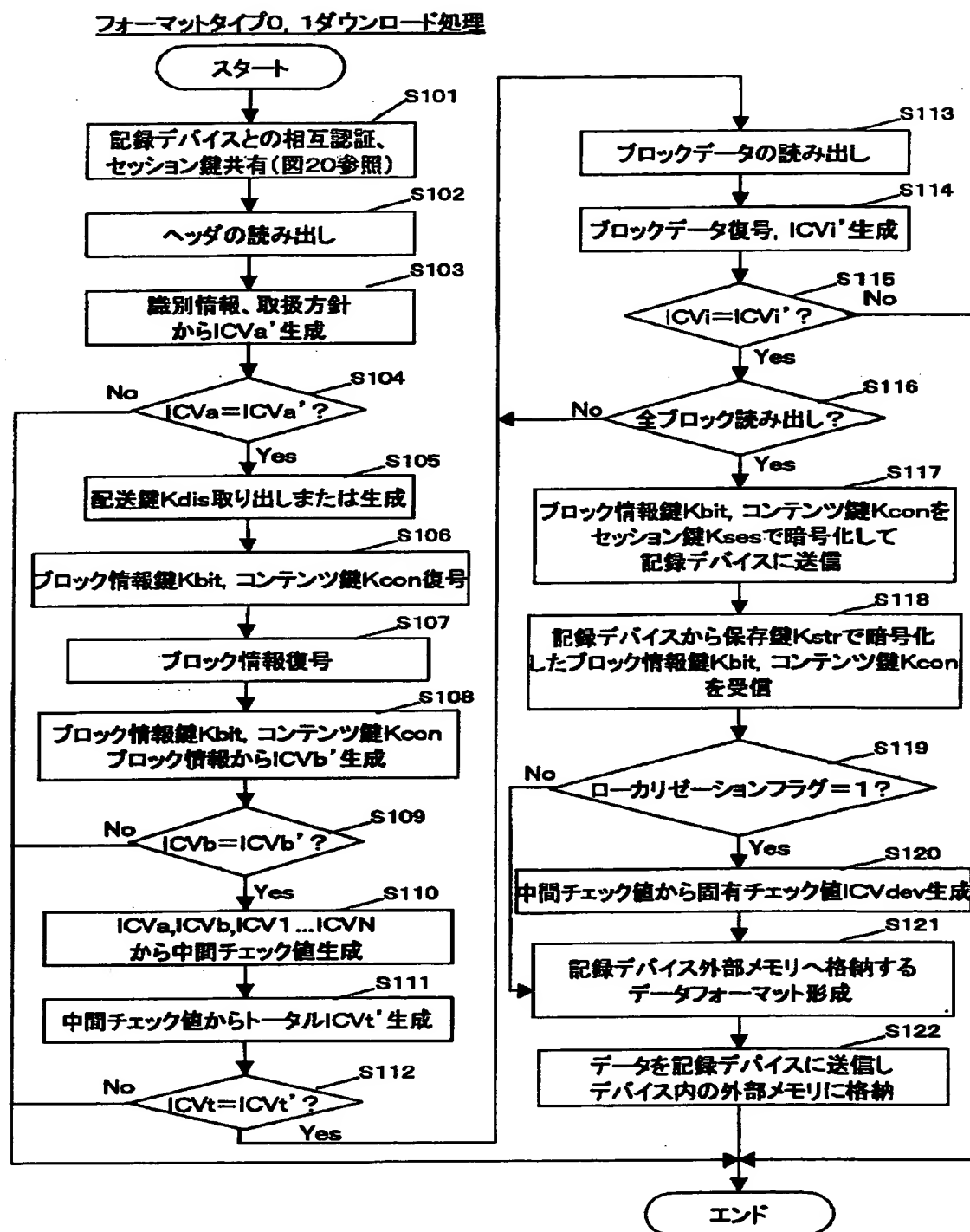
【図 3 8】



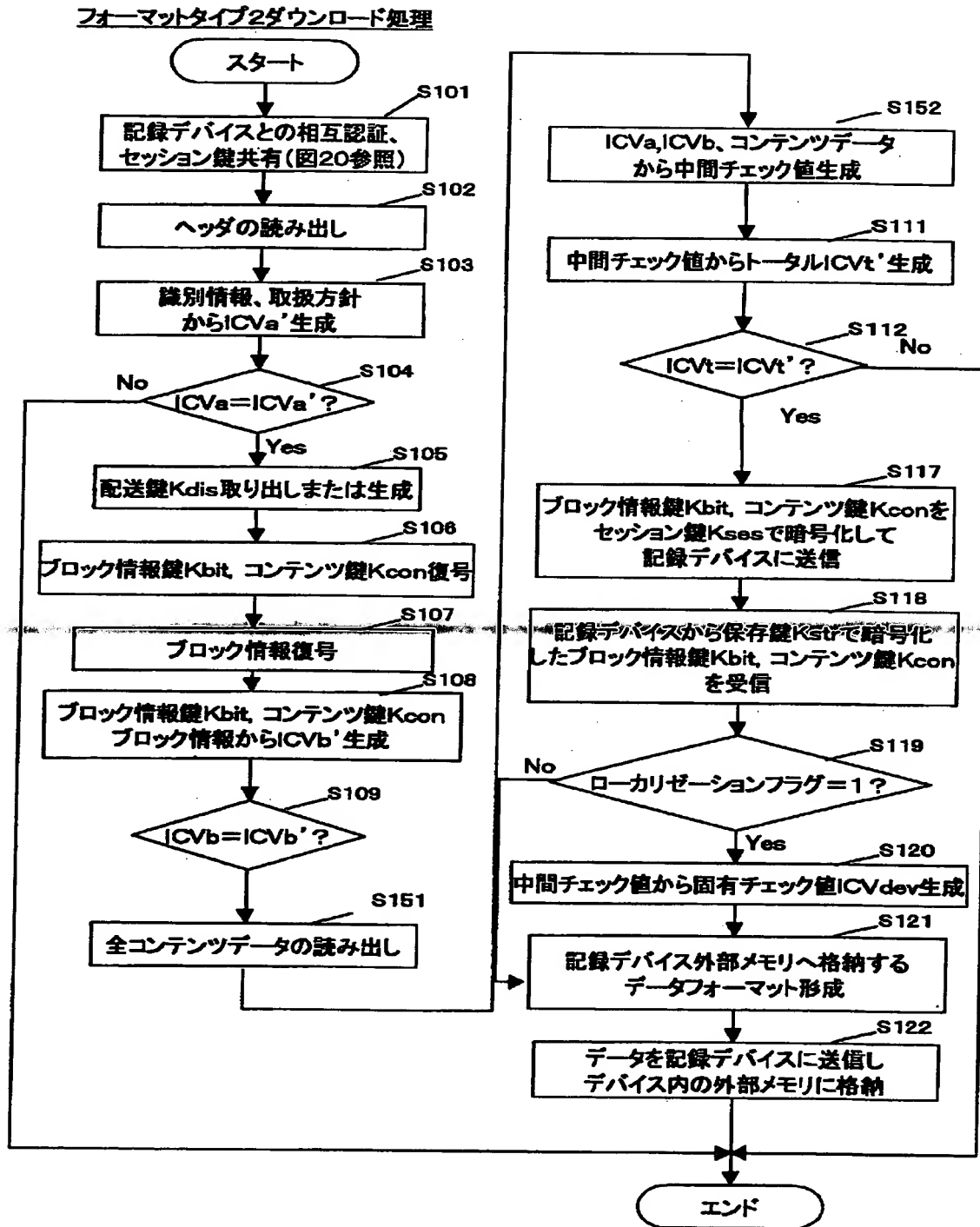
メッセージ $M_1 \sim M_N$: コンテンツブロック 1 ~ N のデータ

⊕ : 排他的論理和処理 (8 バイト単位)

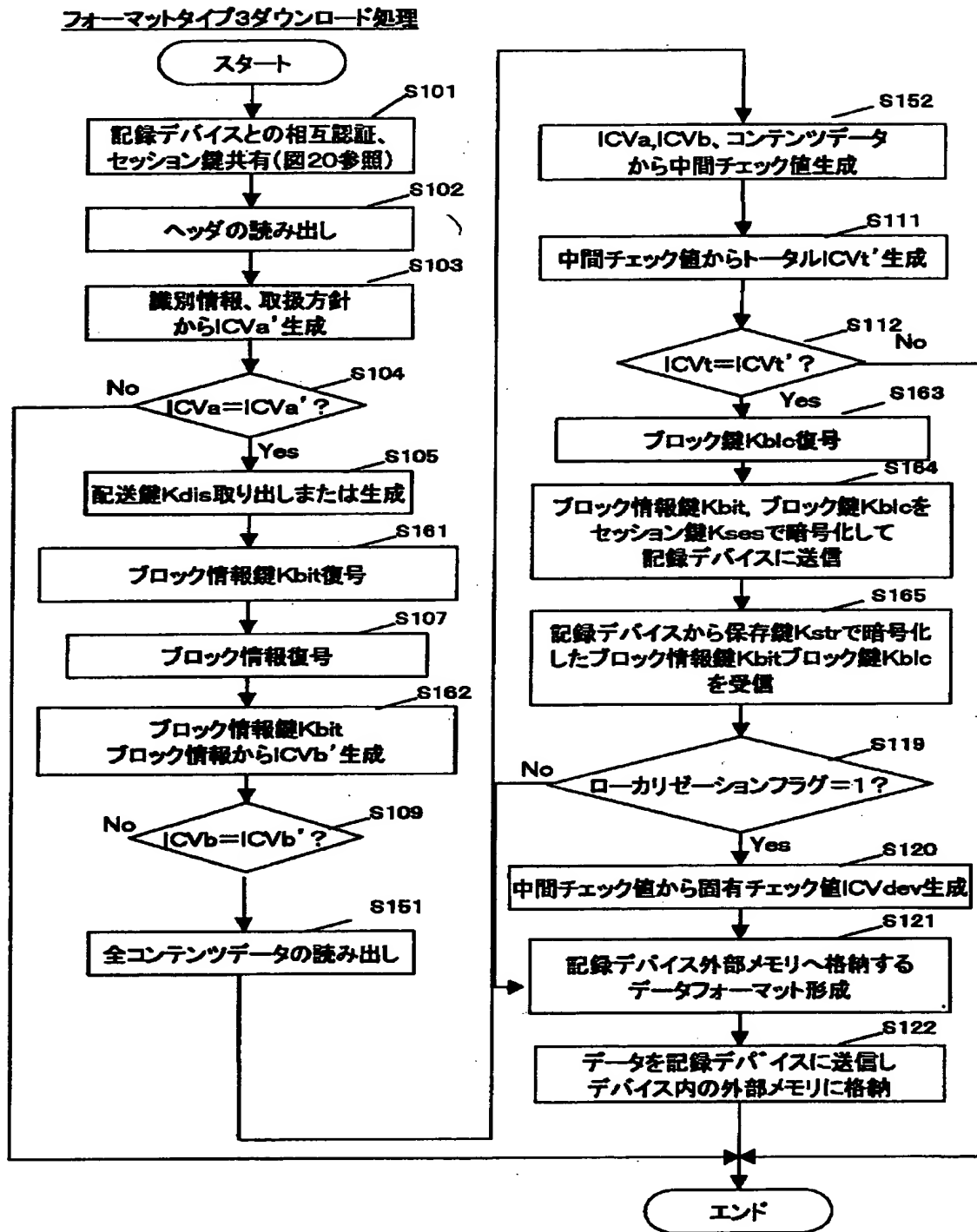
【図39】



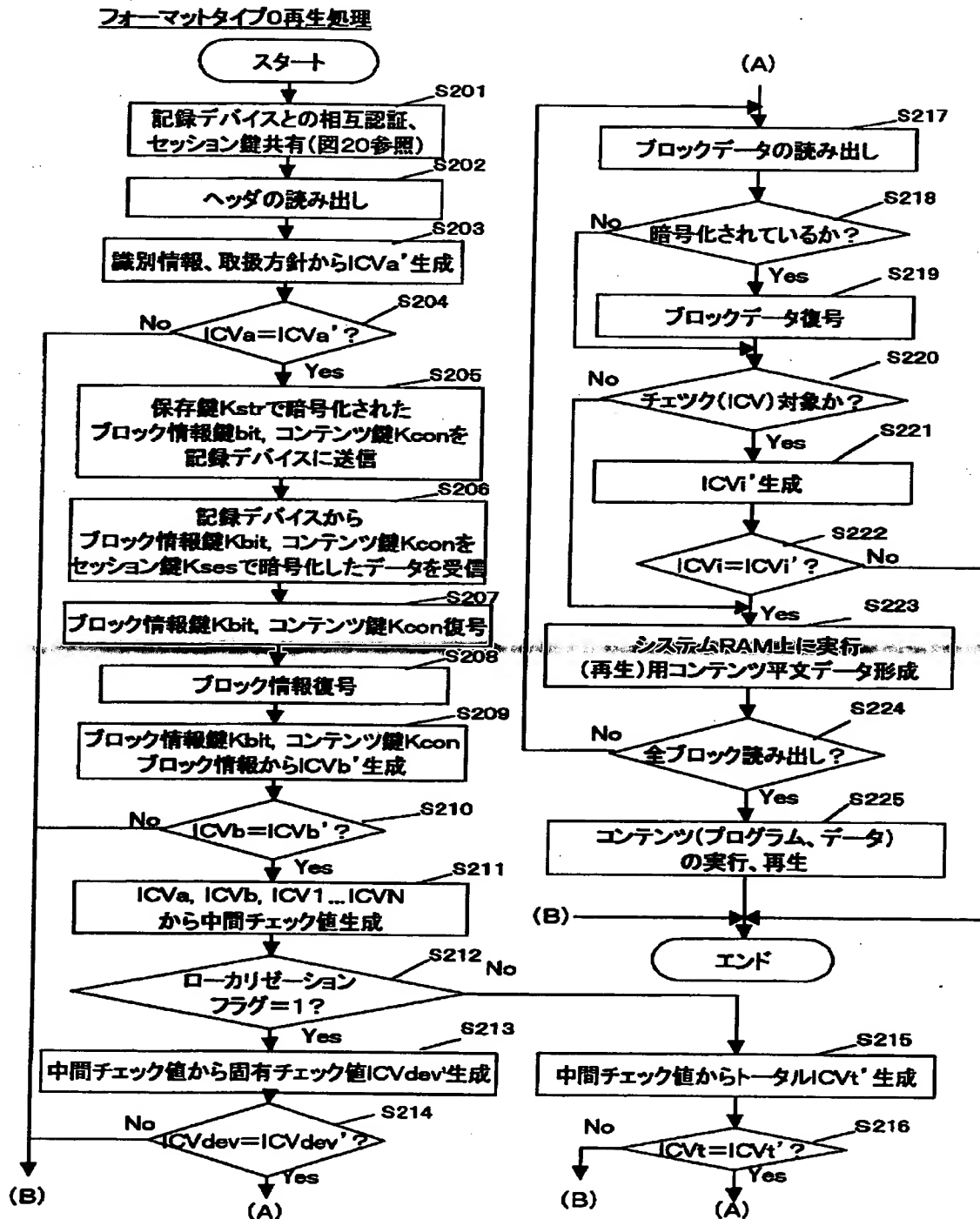
【図40】



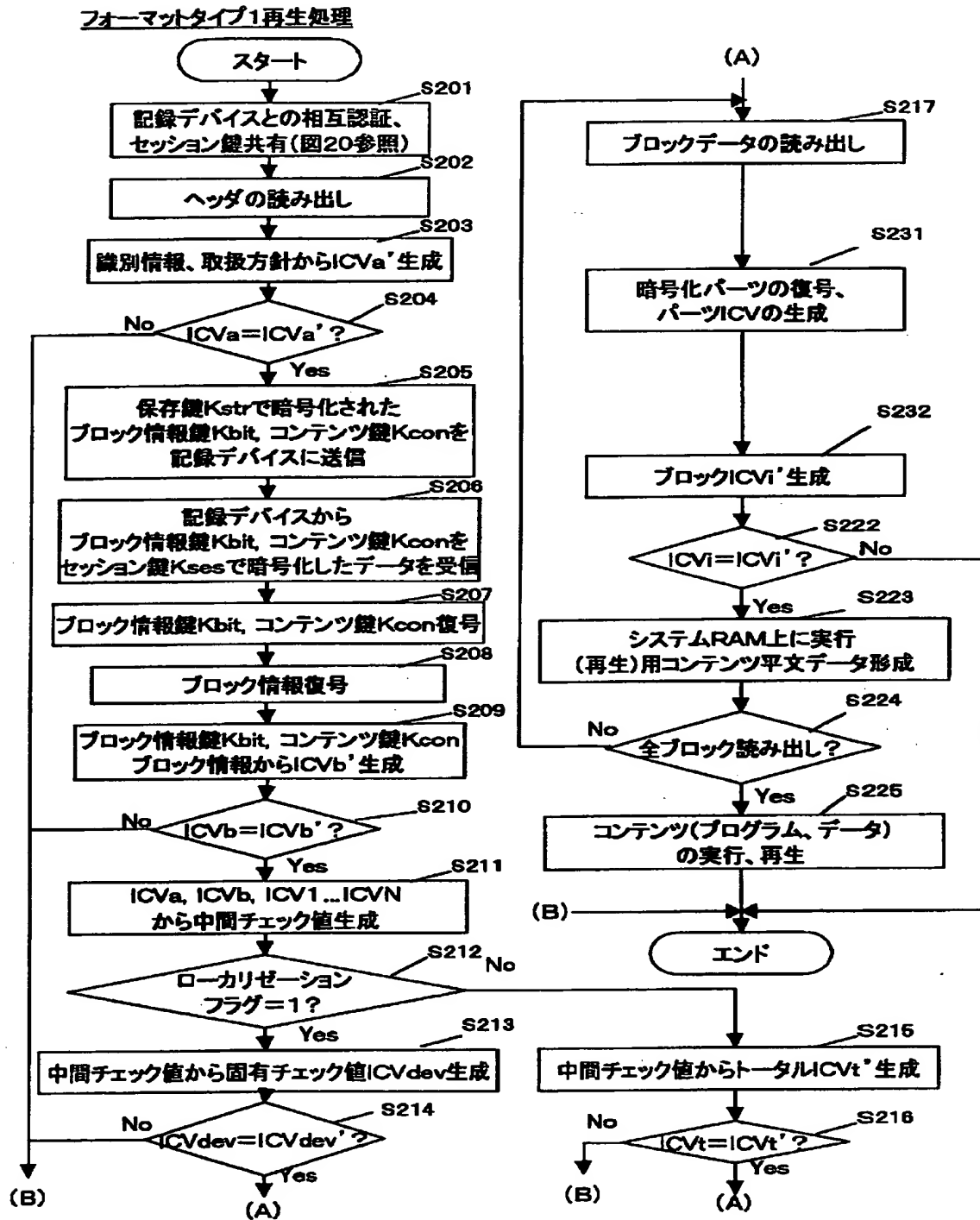
【図 4 1】



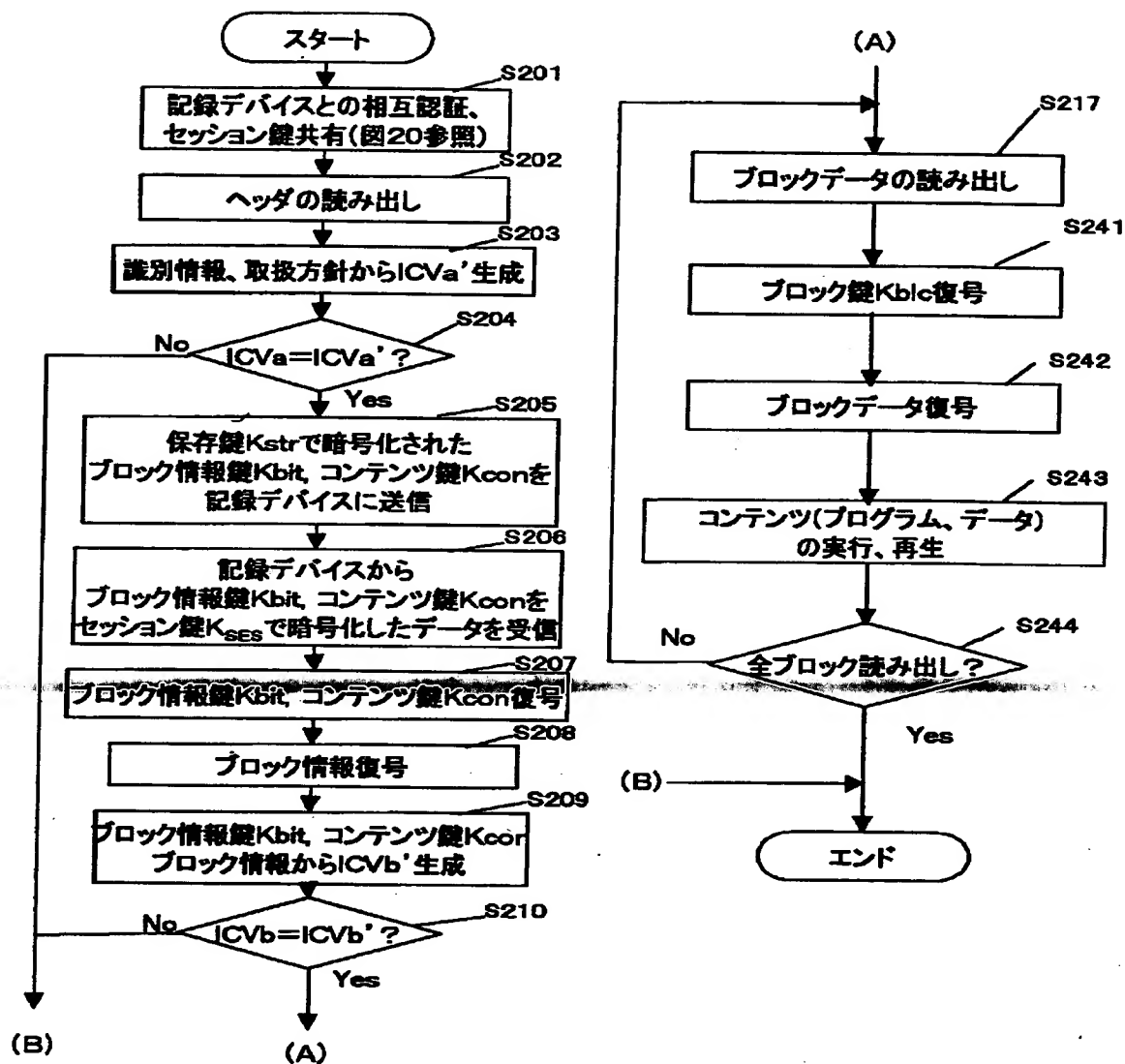
【図42】



【図 43】

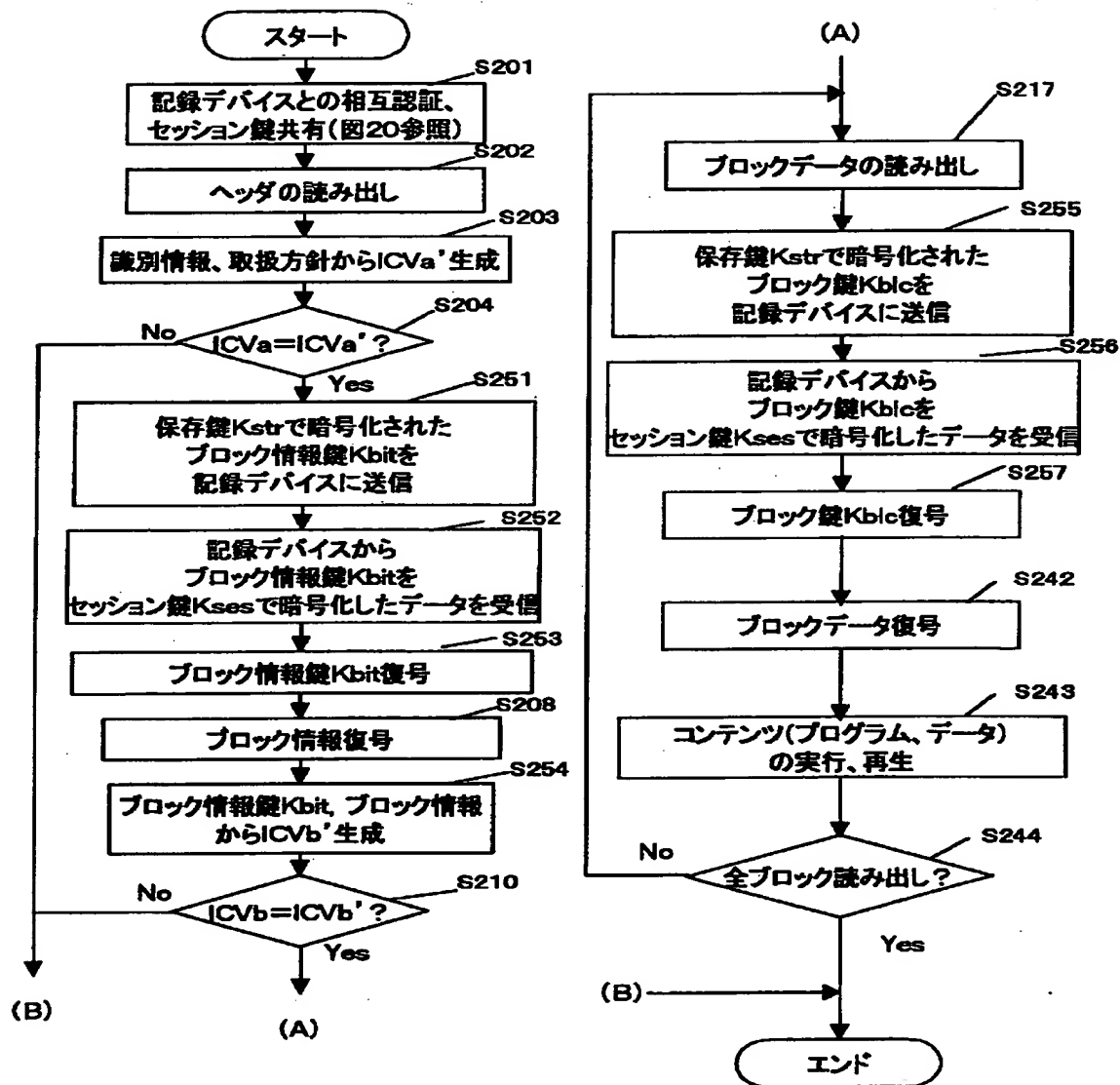


【図44】

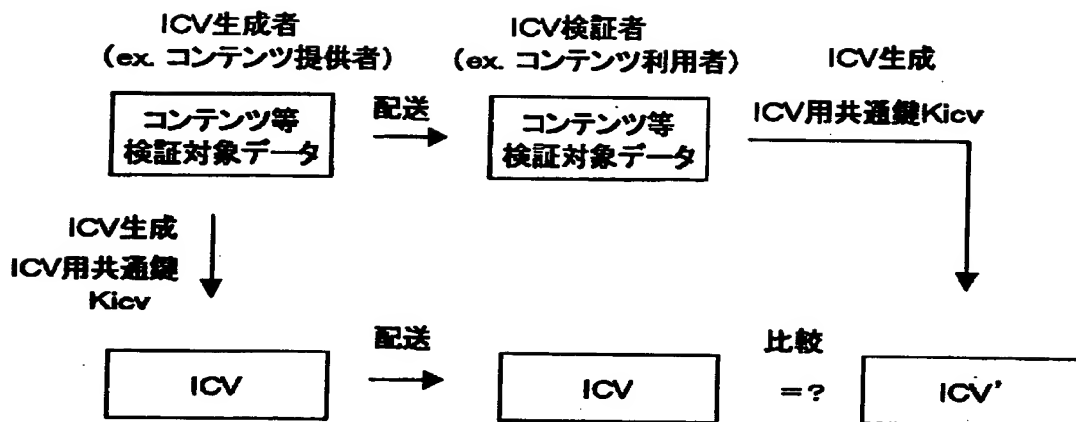


【図 45】

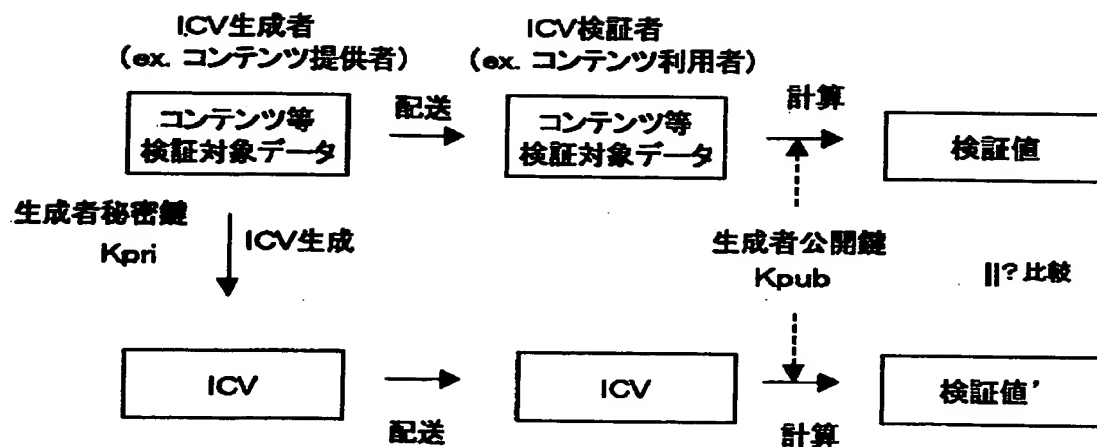
フォーマットタイプ3再生処理



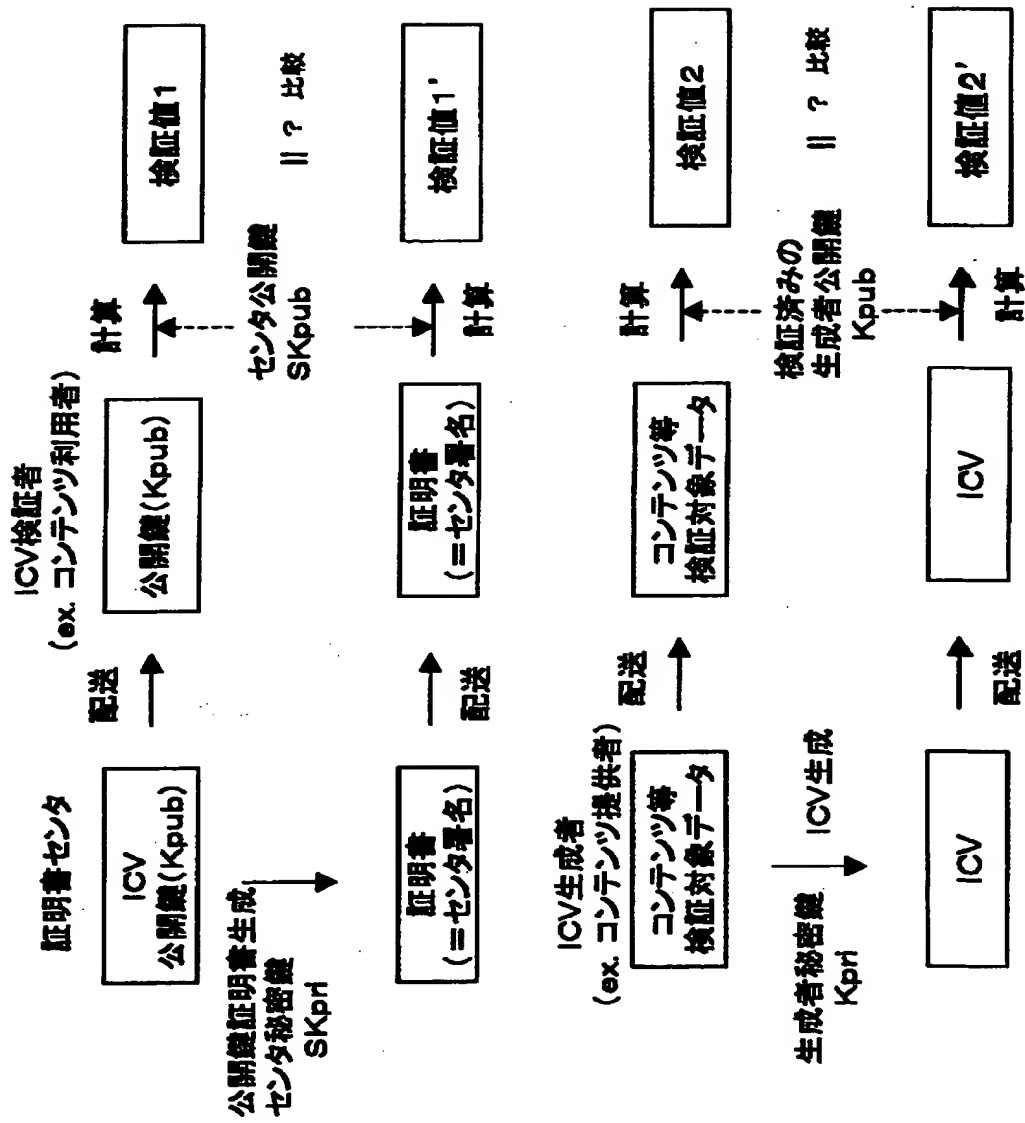
【図 4 6】



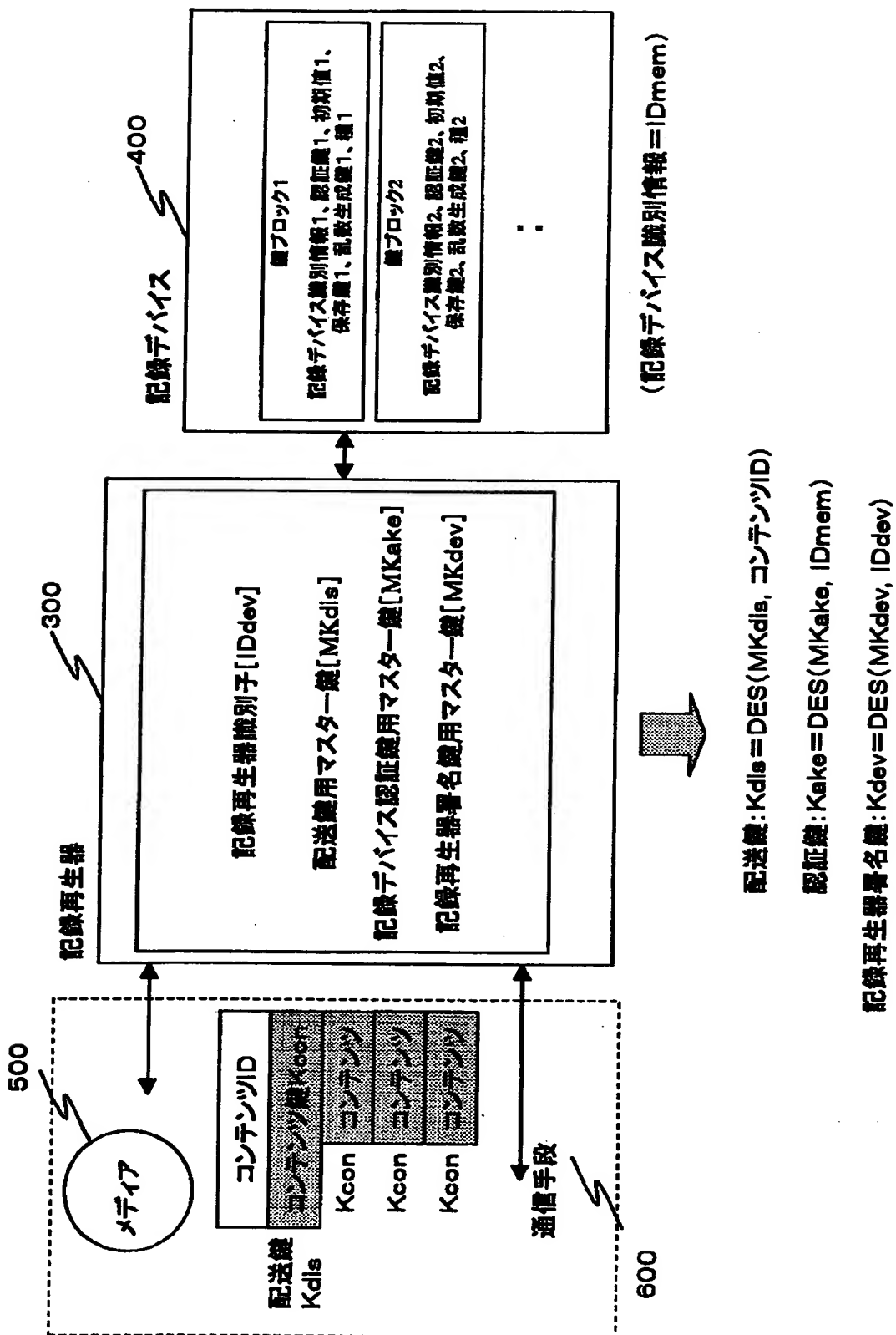
【図 4 7】



【図 48】



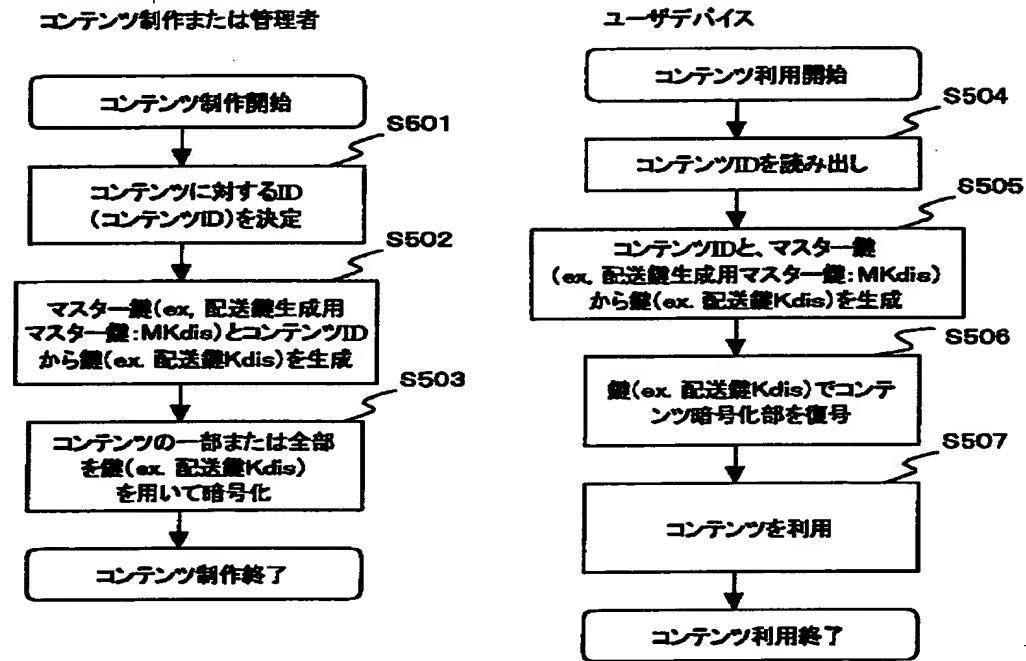
【図 49】



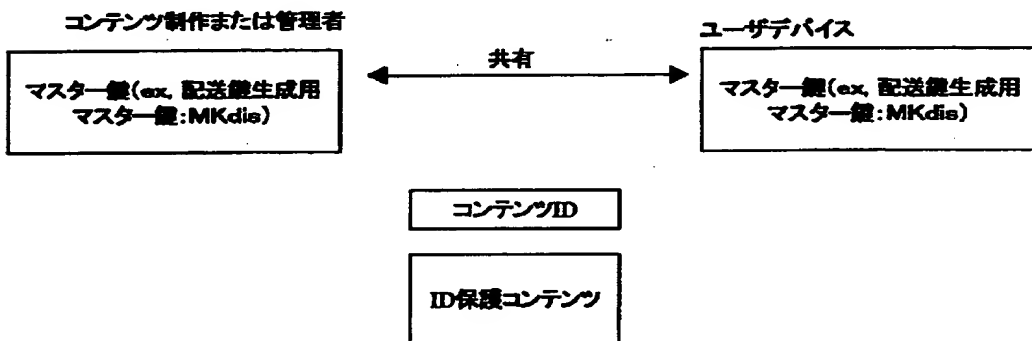
【図50】

Master鍵から個別の鍵を生成する方法-(1)

【基本フロー】



【鍵所有構成】

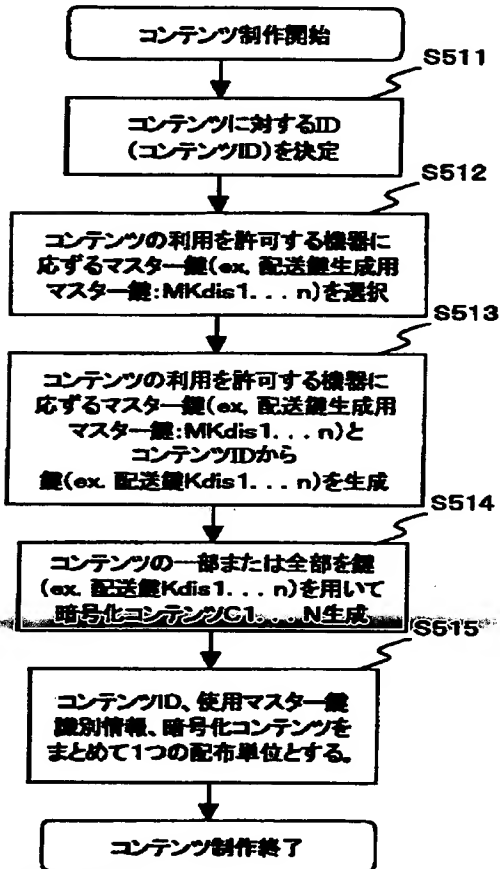


【図51】

Master鍵から個別の鍵を生成する方法-(2)

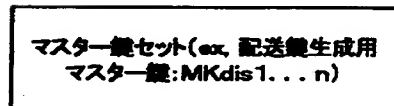
【基本フロー】

コンテンツ制作または管理者

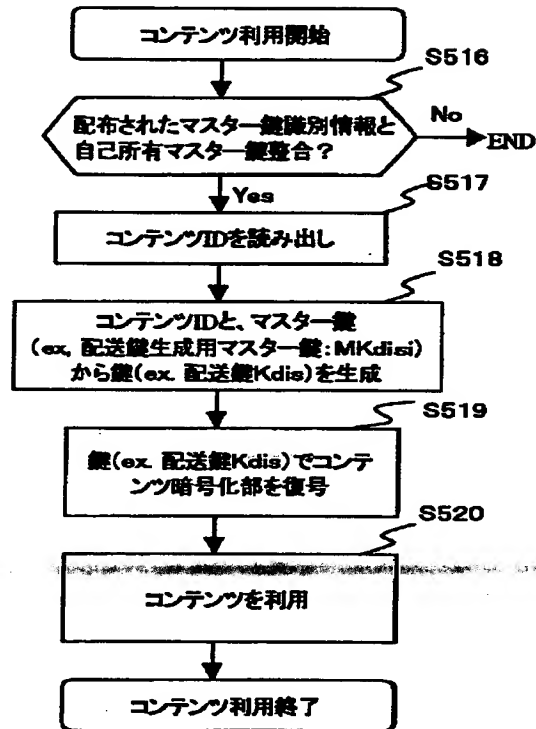


【鍵所有構成】

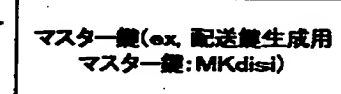
コンテンツ制作または管理者



ユーザデバイス



ユーザデバイス

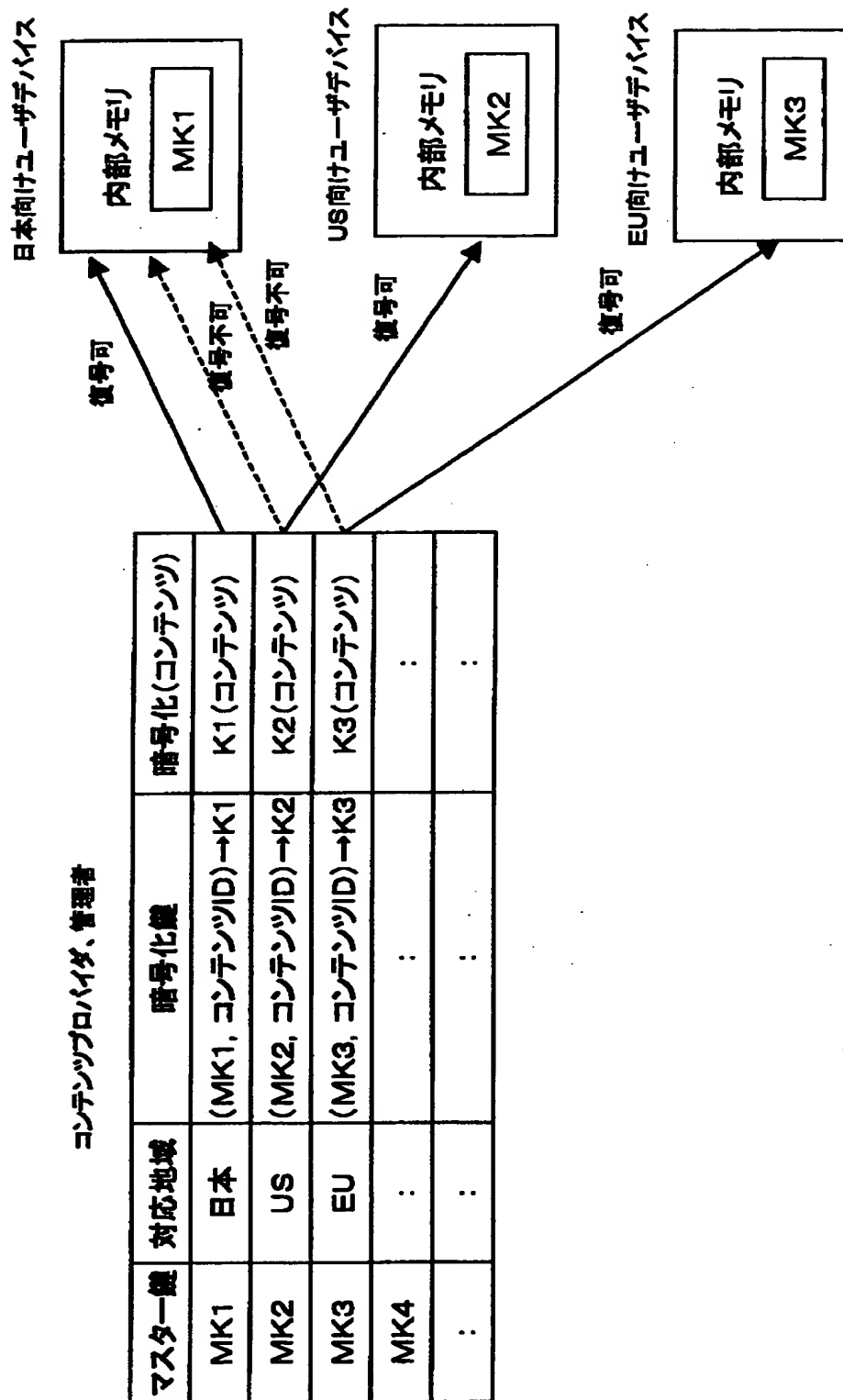


共有

コンテンツID

ID保護コンテンツ

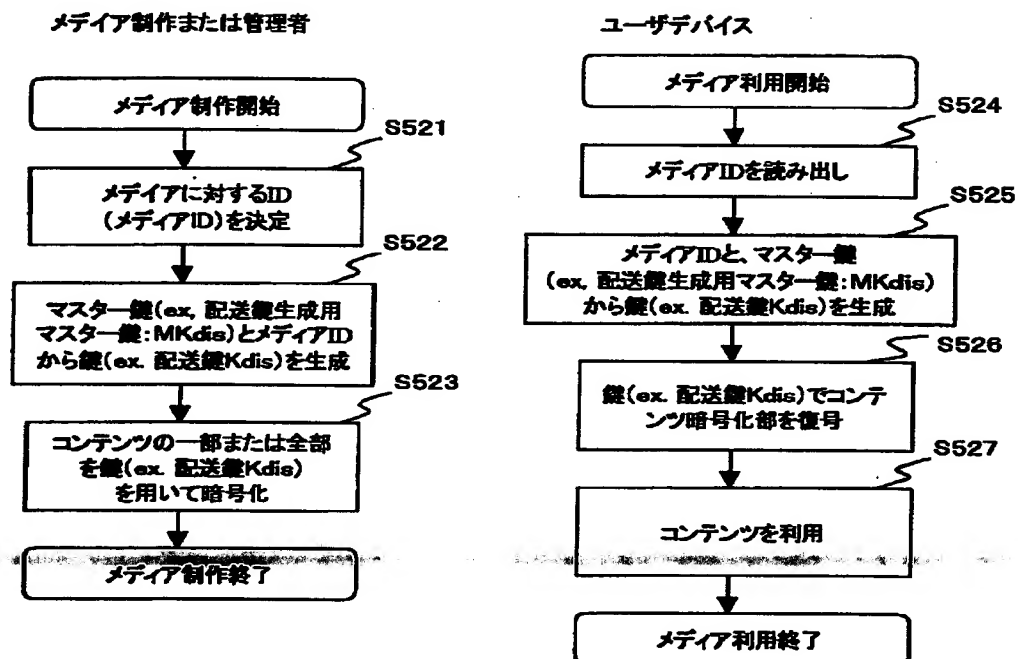
【図 5 2】



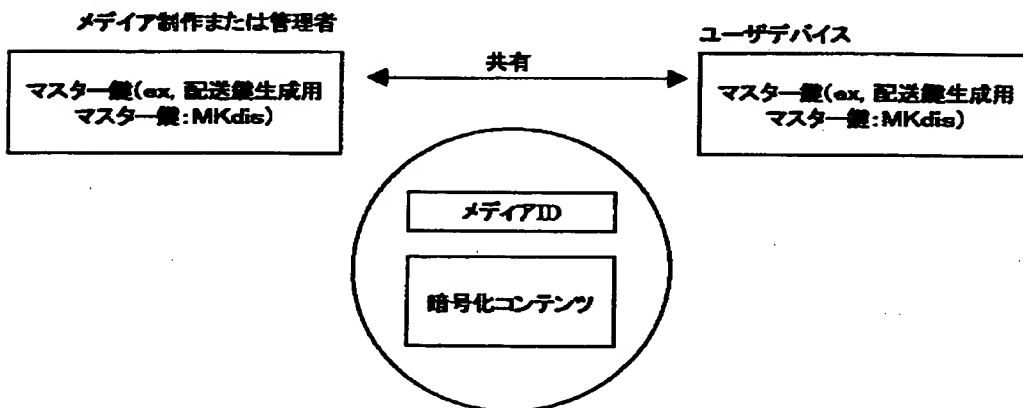
【図53】

Master鍵から個別の鍵を生成する方法-(3)

【基本フロー】



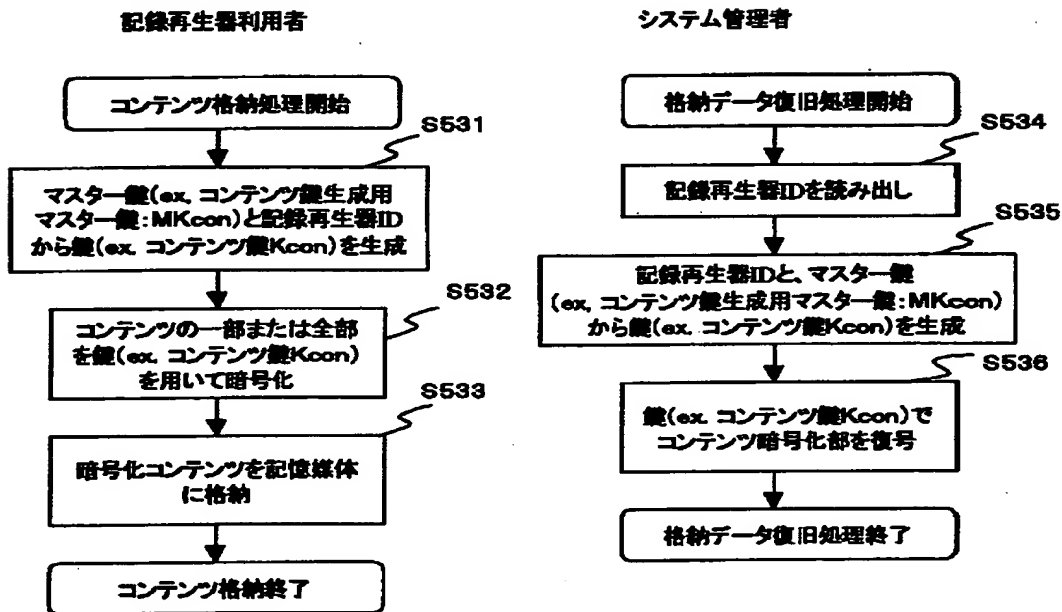
【鍵所有構成】



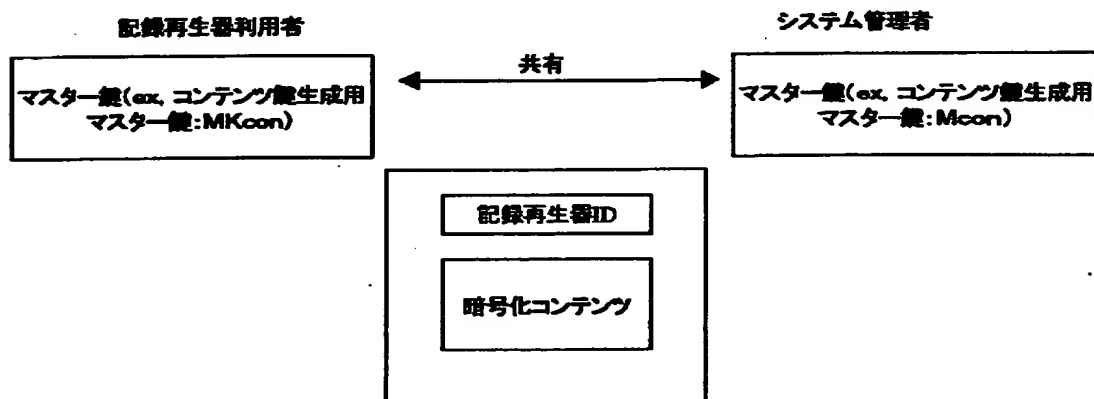
【図54】

Master鍵から個別の鍵を生成する方法-(4)

【基本フロー】



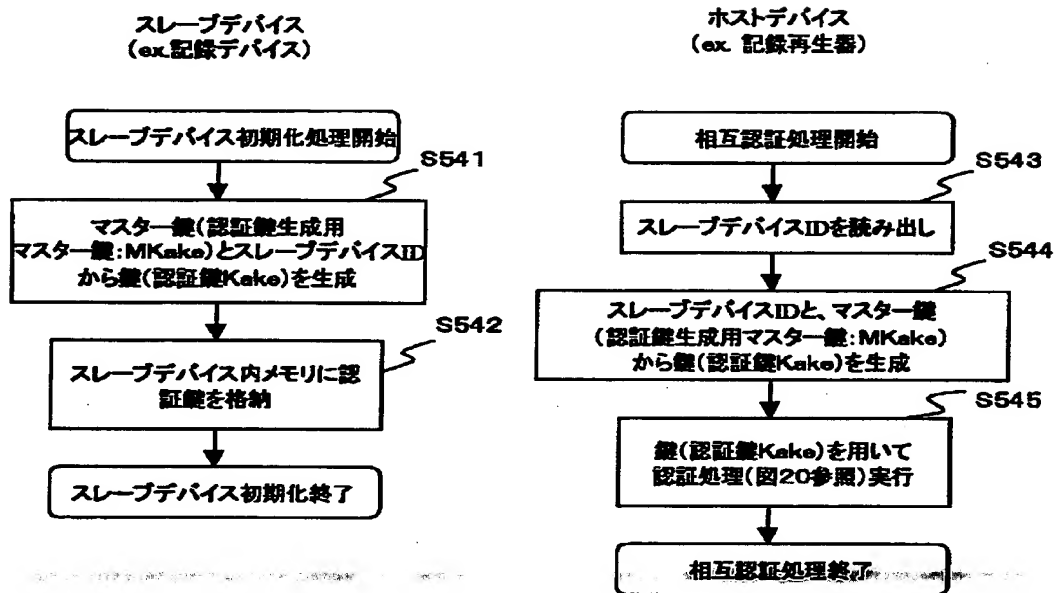
【鍵所有構成】



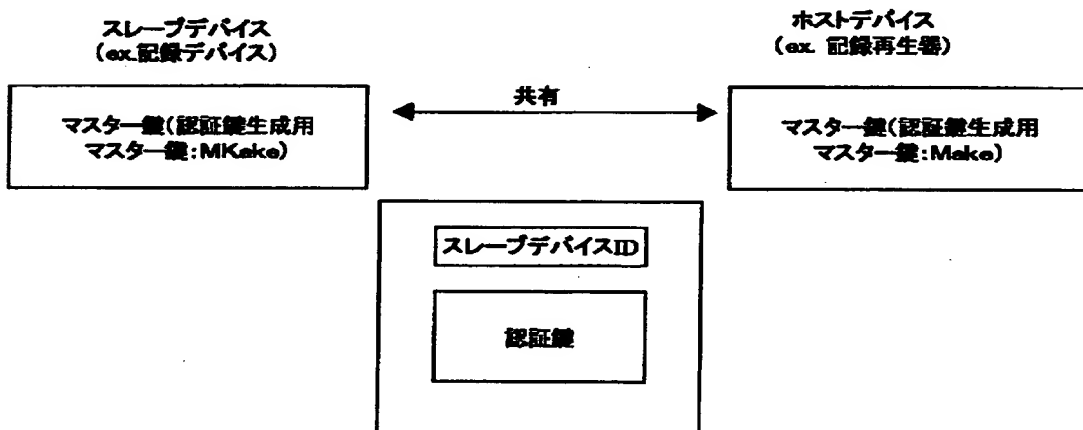
【図 5 5】

Master鍵から個別の鍵を生成する方法-(5)

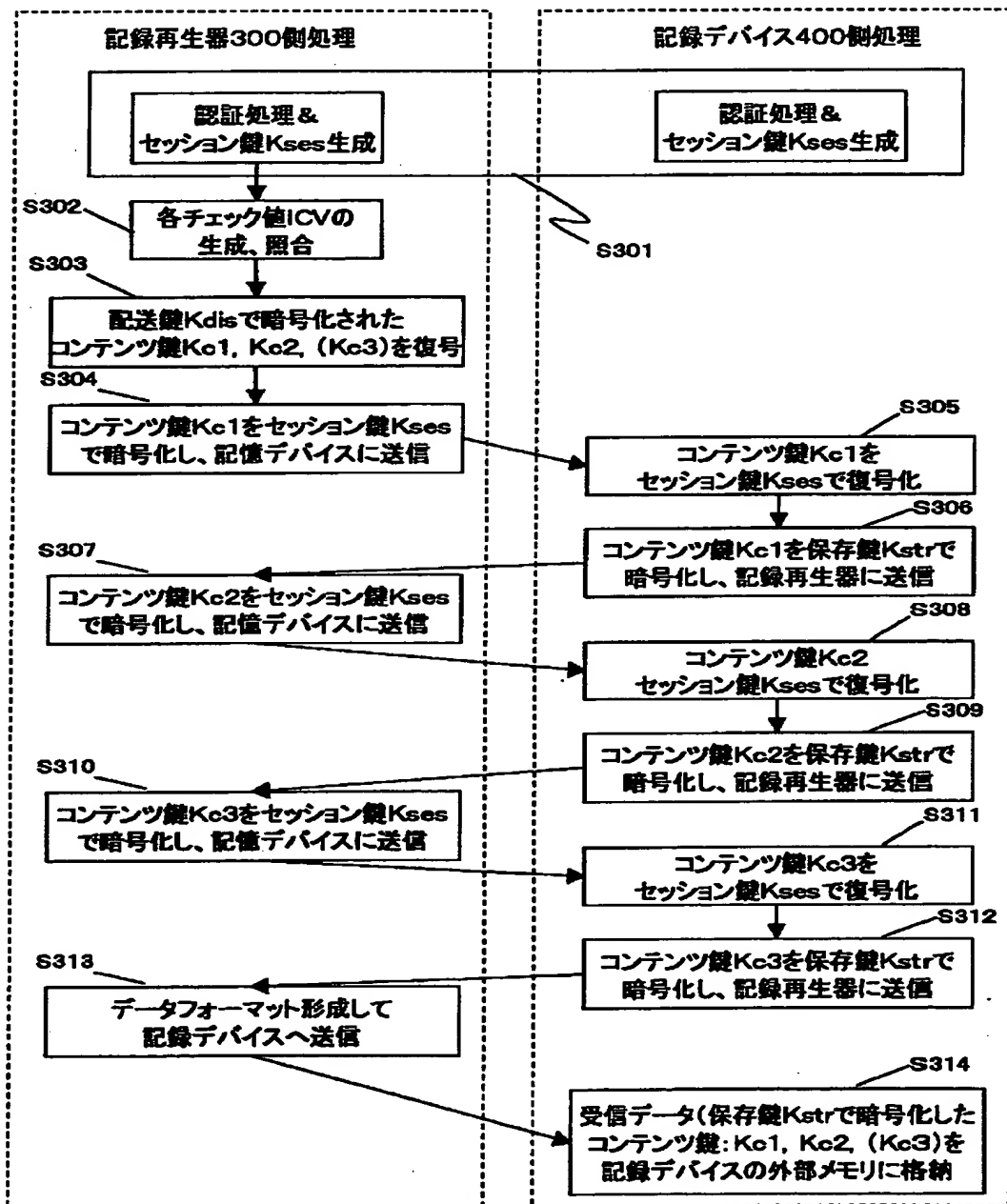
【基本フロー】



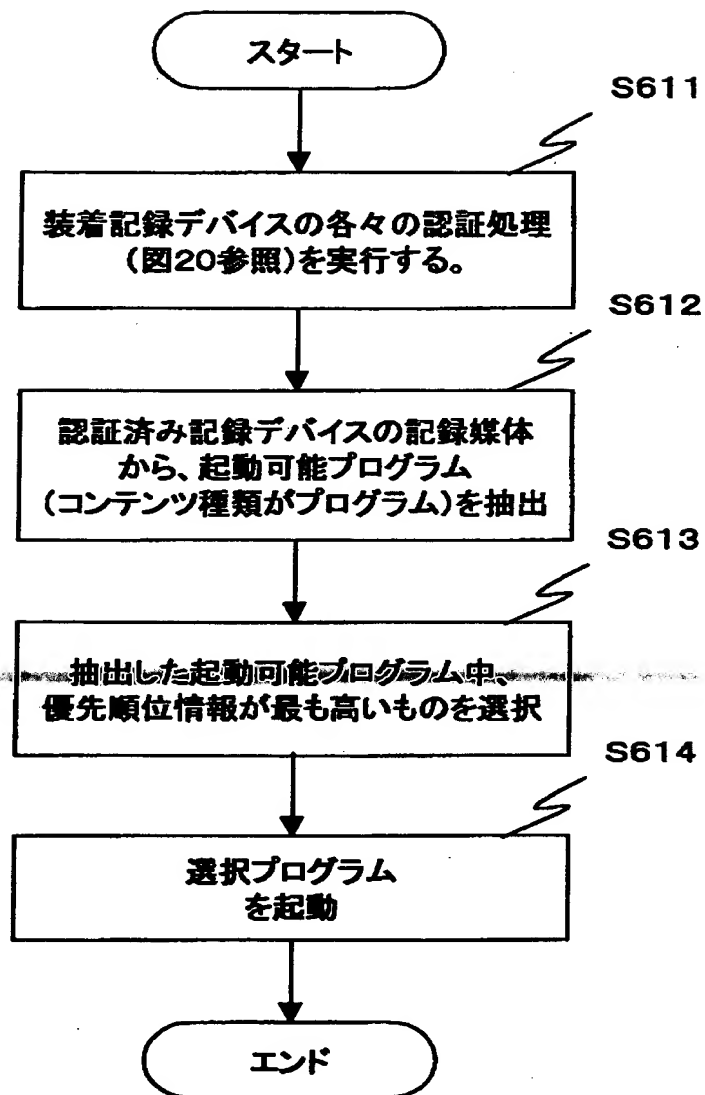
【鍵所有構成】



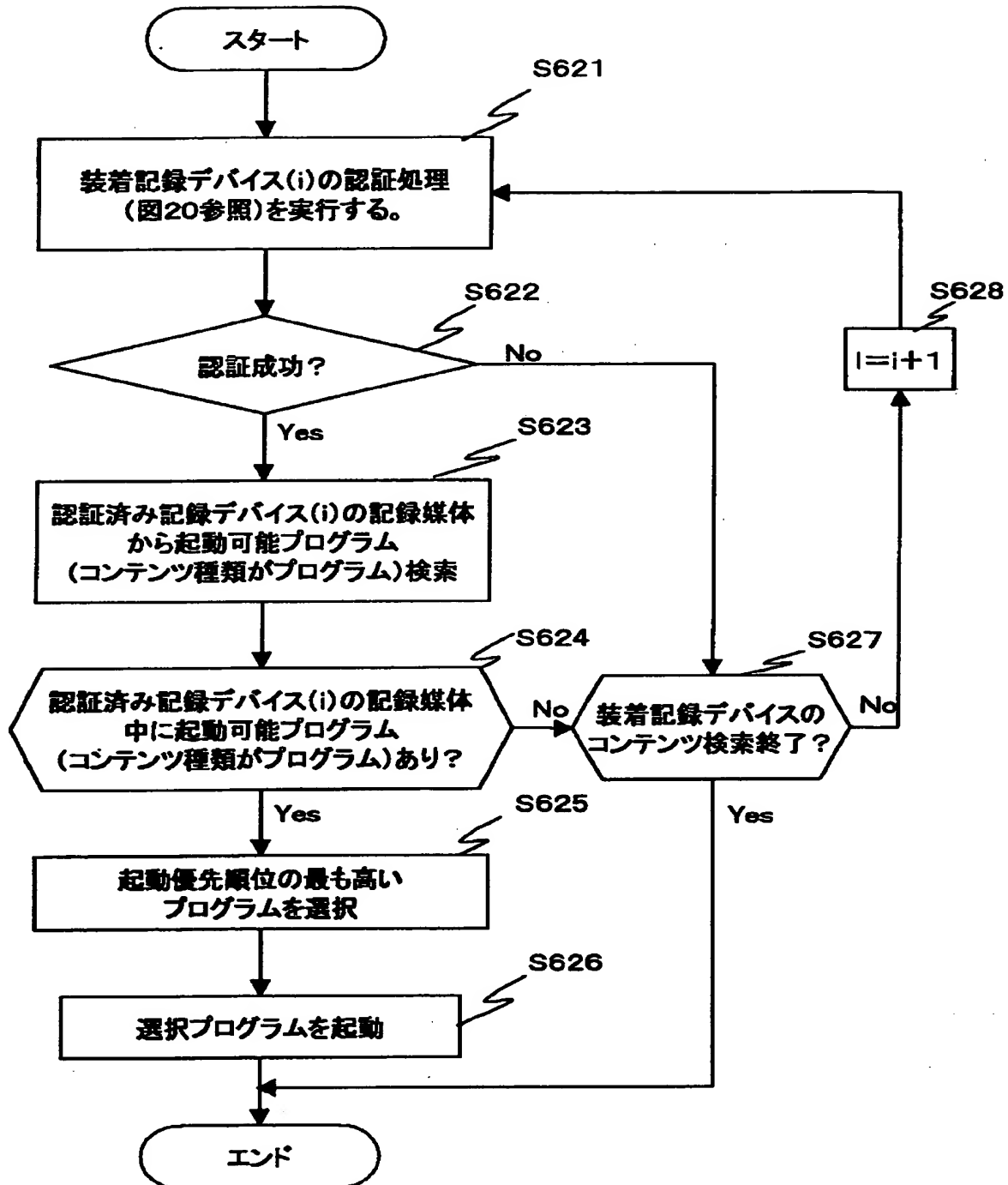
【図56】

トリプルDES適用コンテンツ鍵: K_{C1} , K_{C2} , (K_{C3}) の格納(ダウンロード)処理

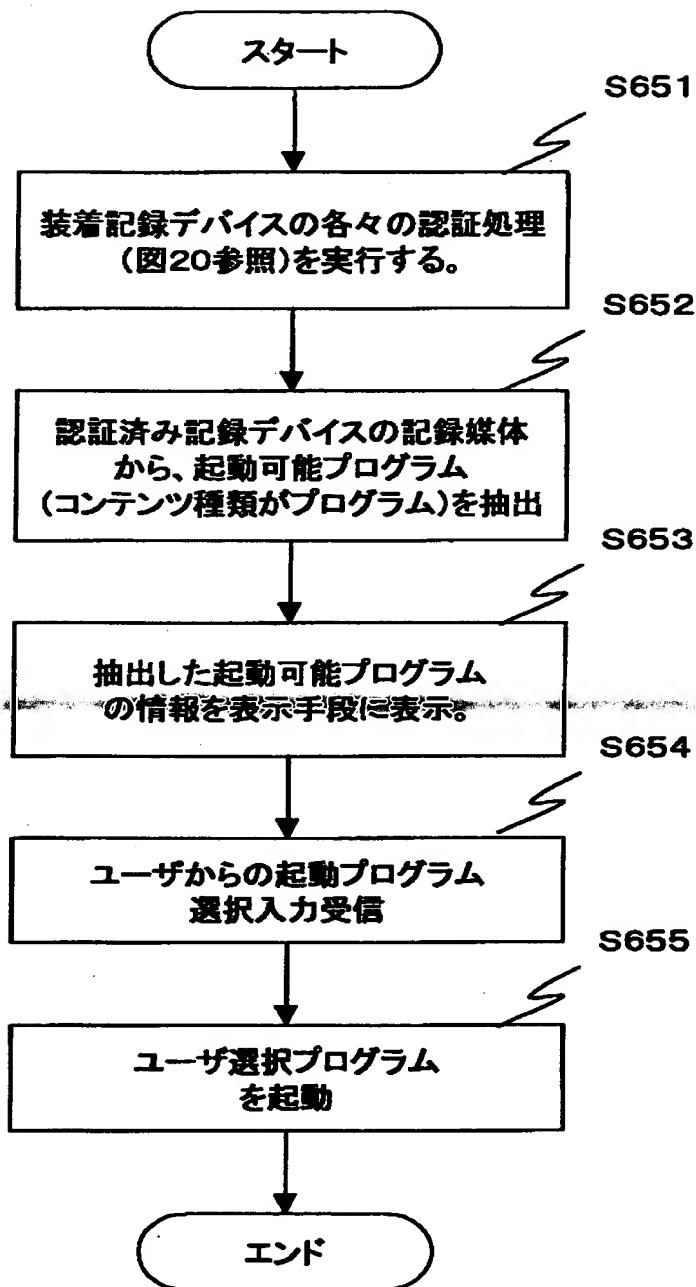
【図 57】



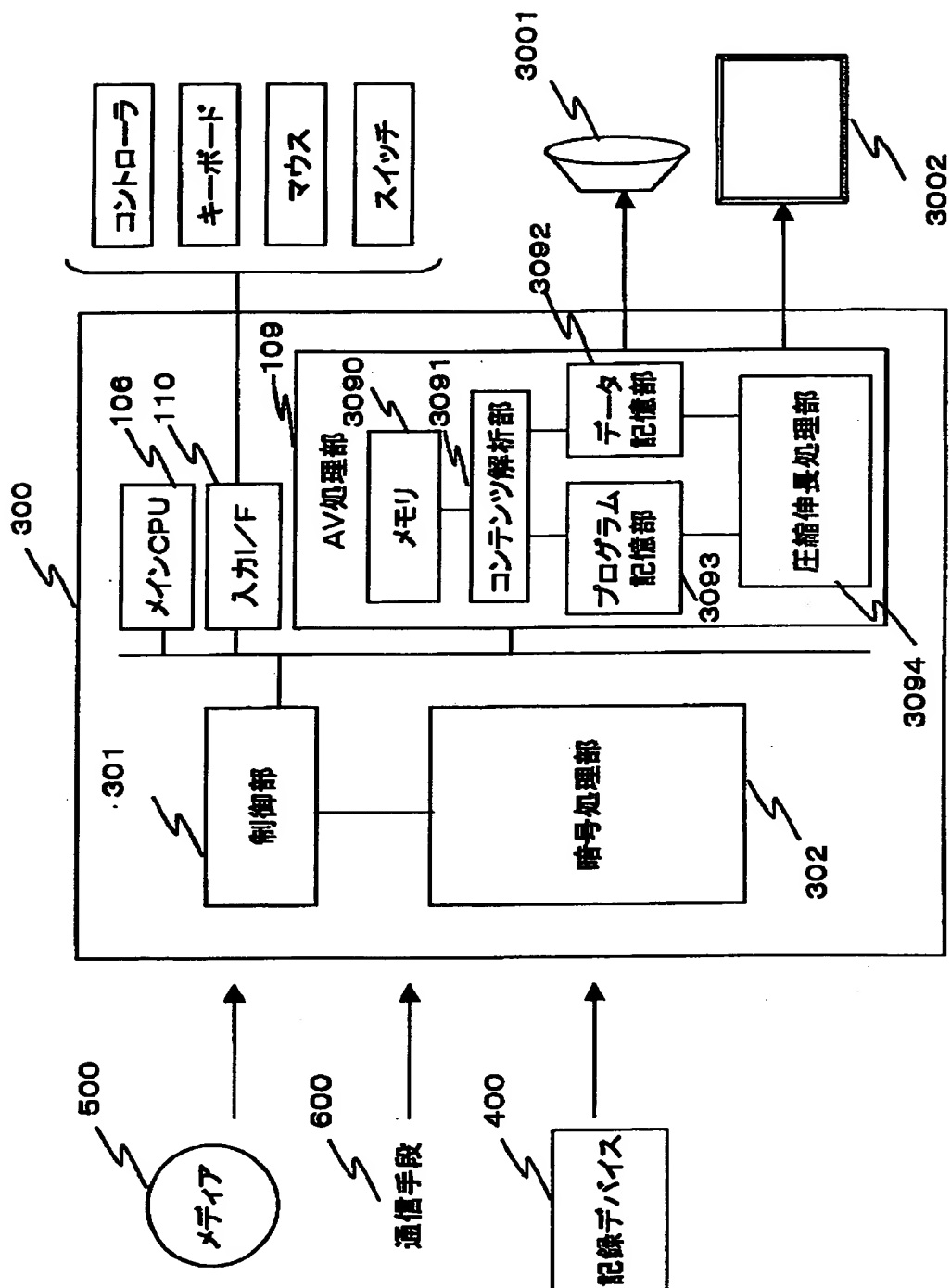
【図 58】



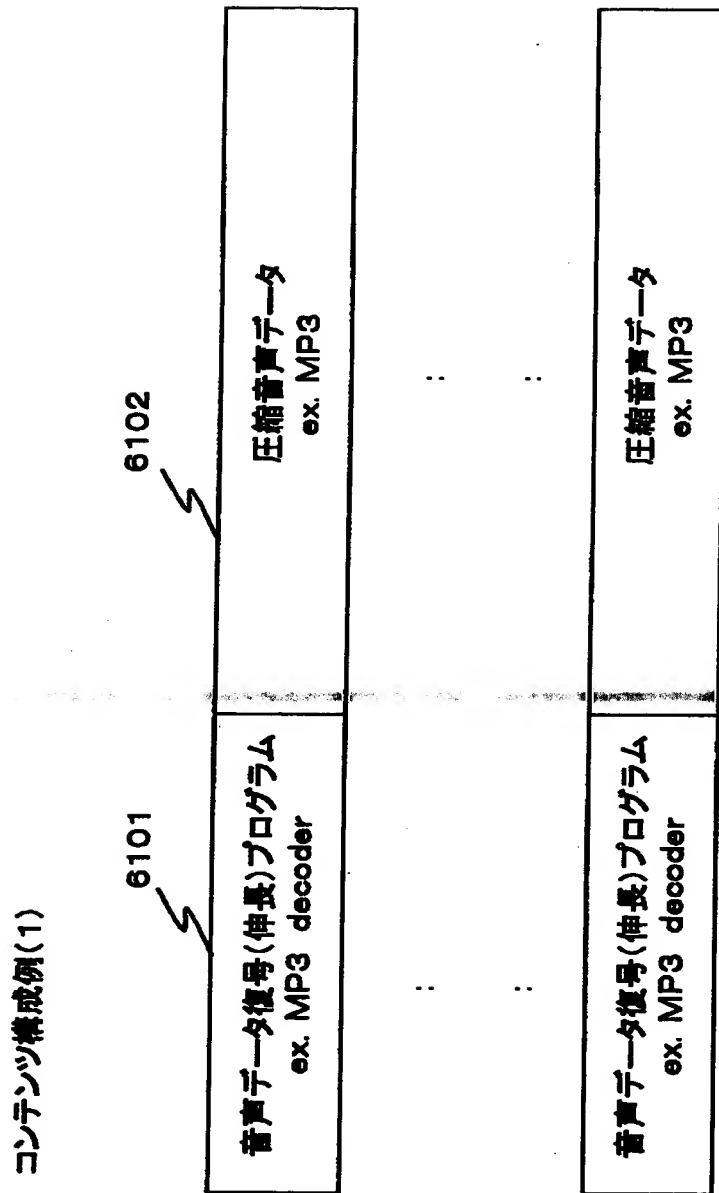
【図59】



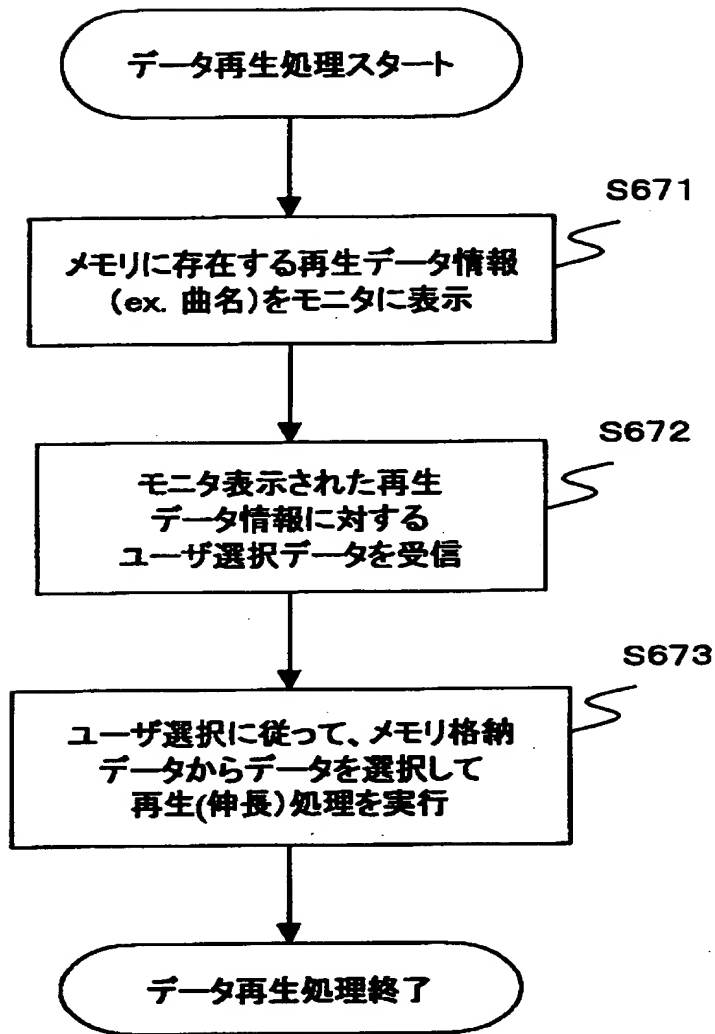
【図60】



【図 6 1】

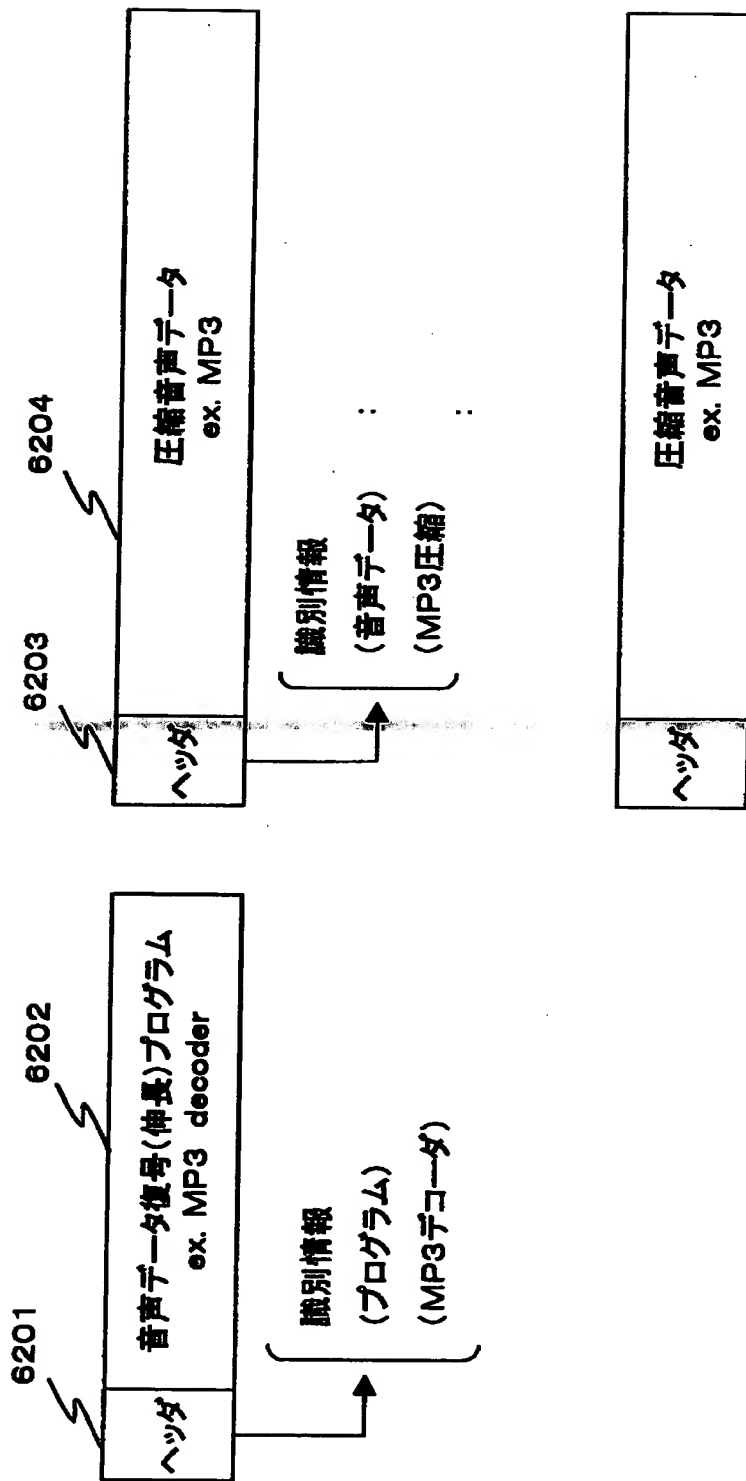


【図 62】

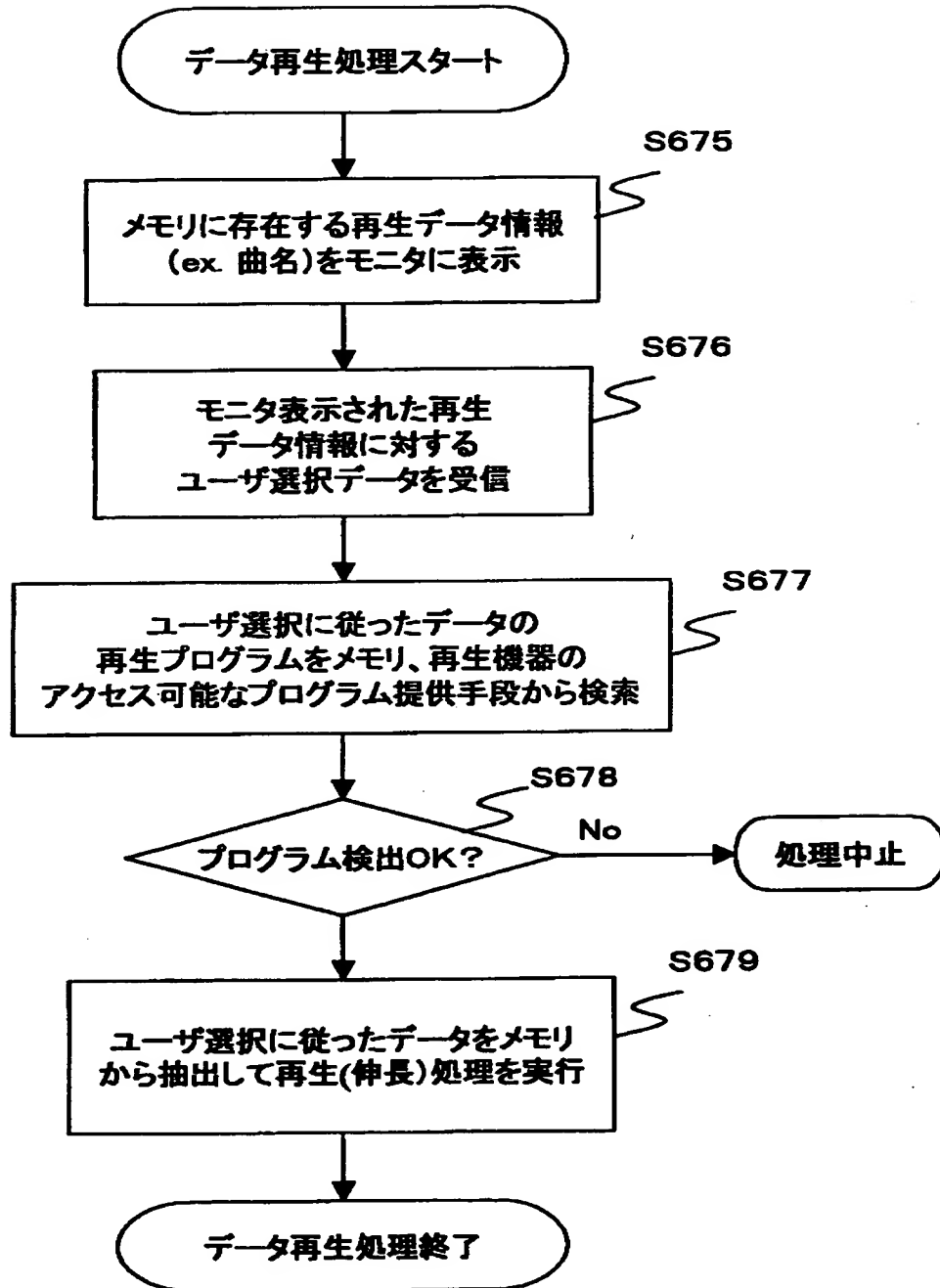


【図 63】

コンテンツ構成例(2)

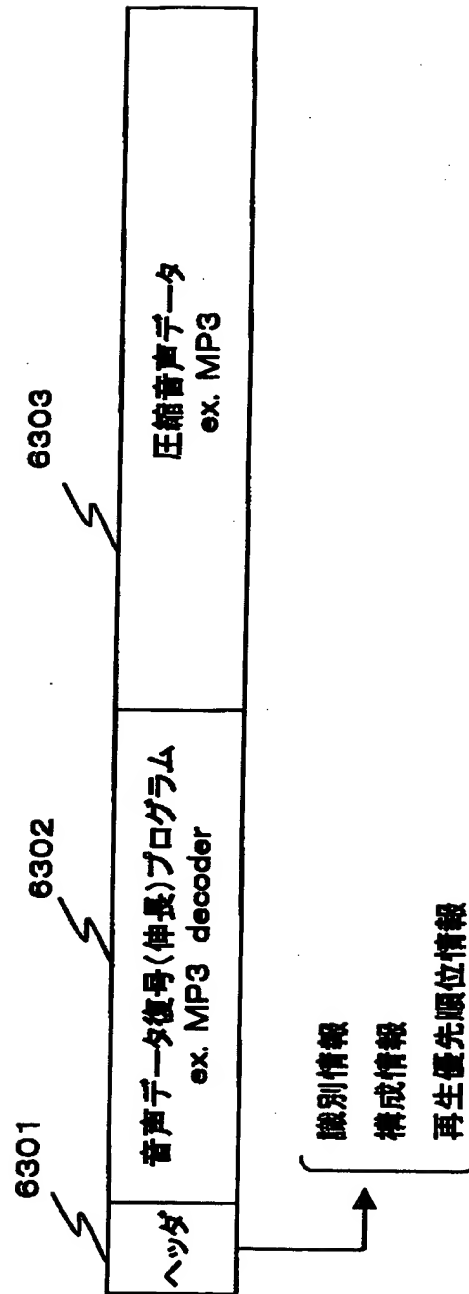


【図 64】

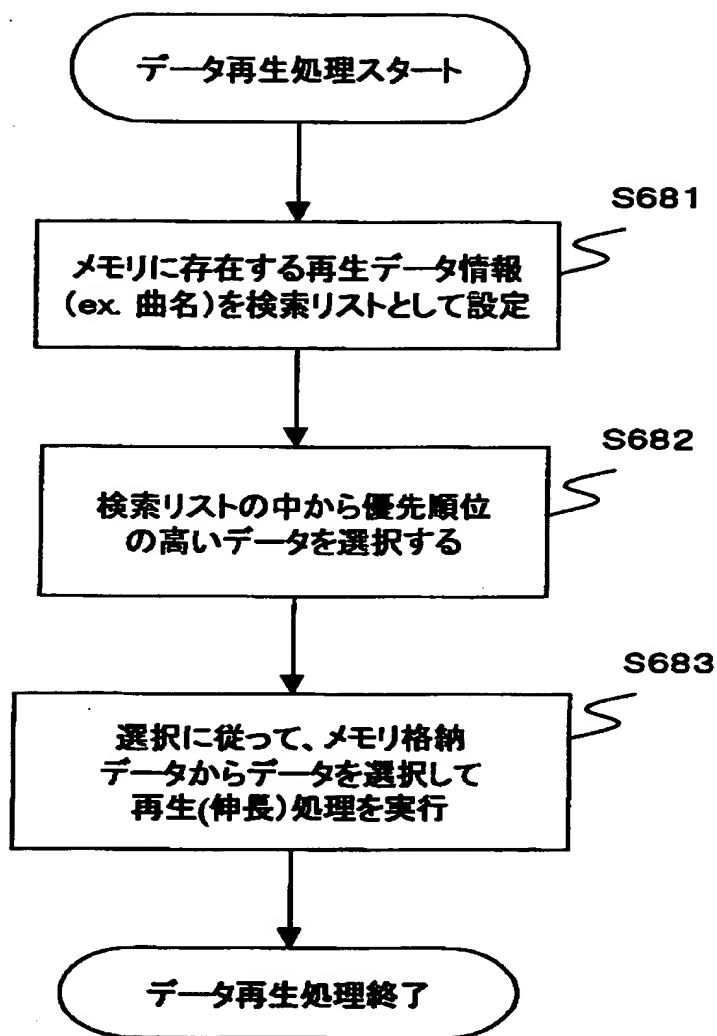


【図 65】

コンテンツ構成例(3)

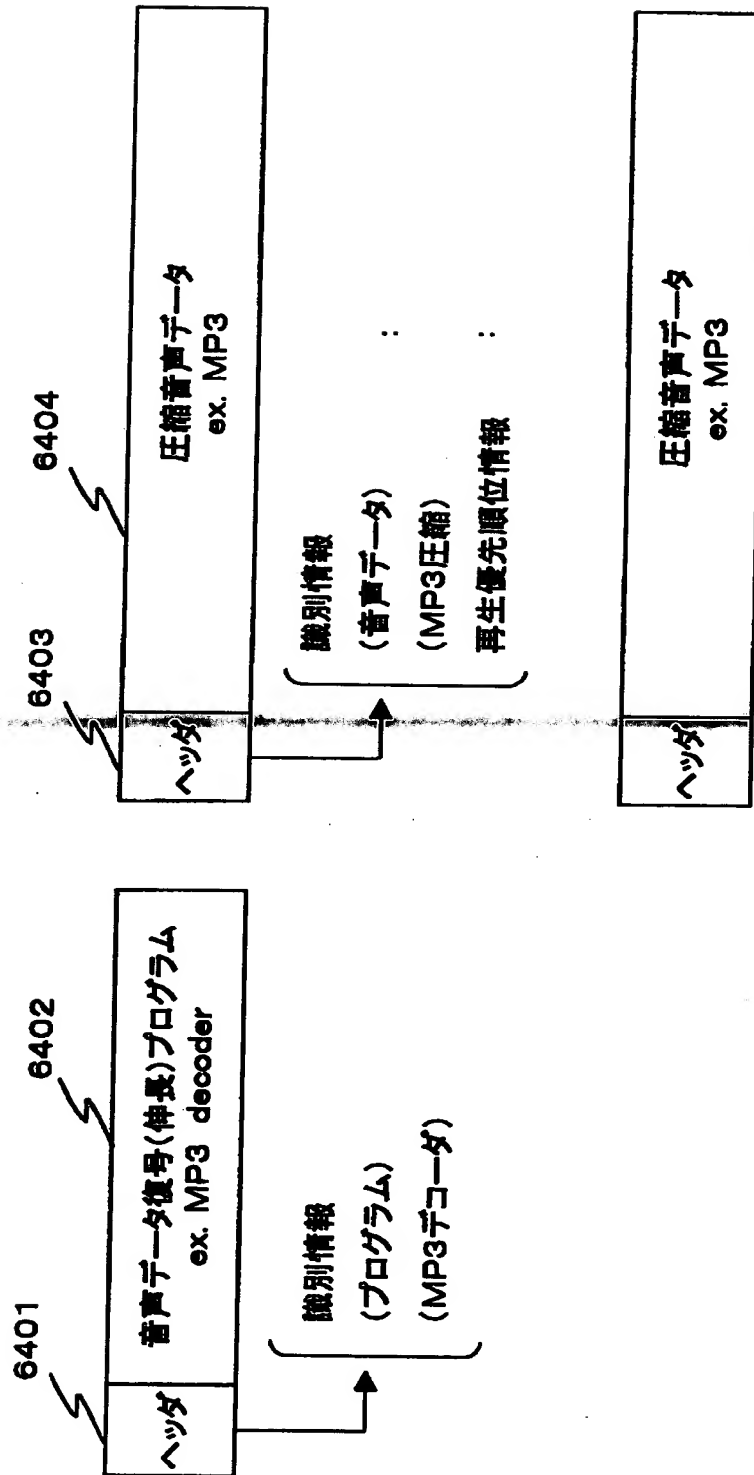


【図 66】

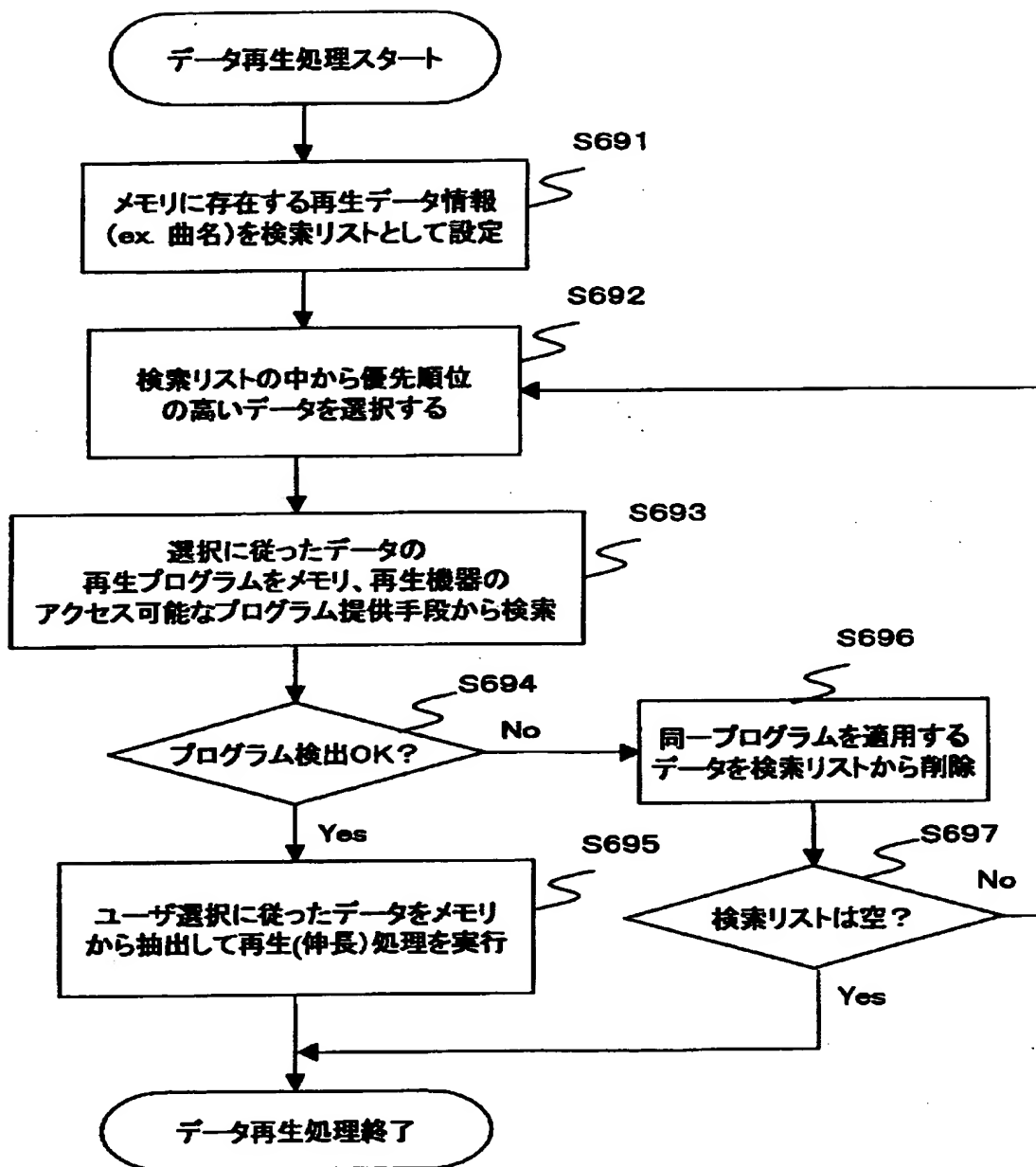


【図 67】

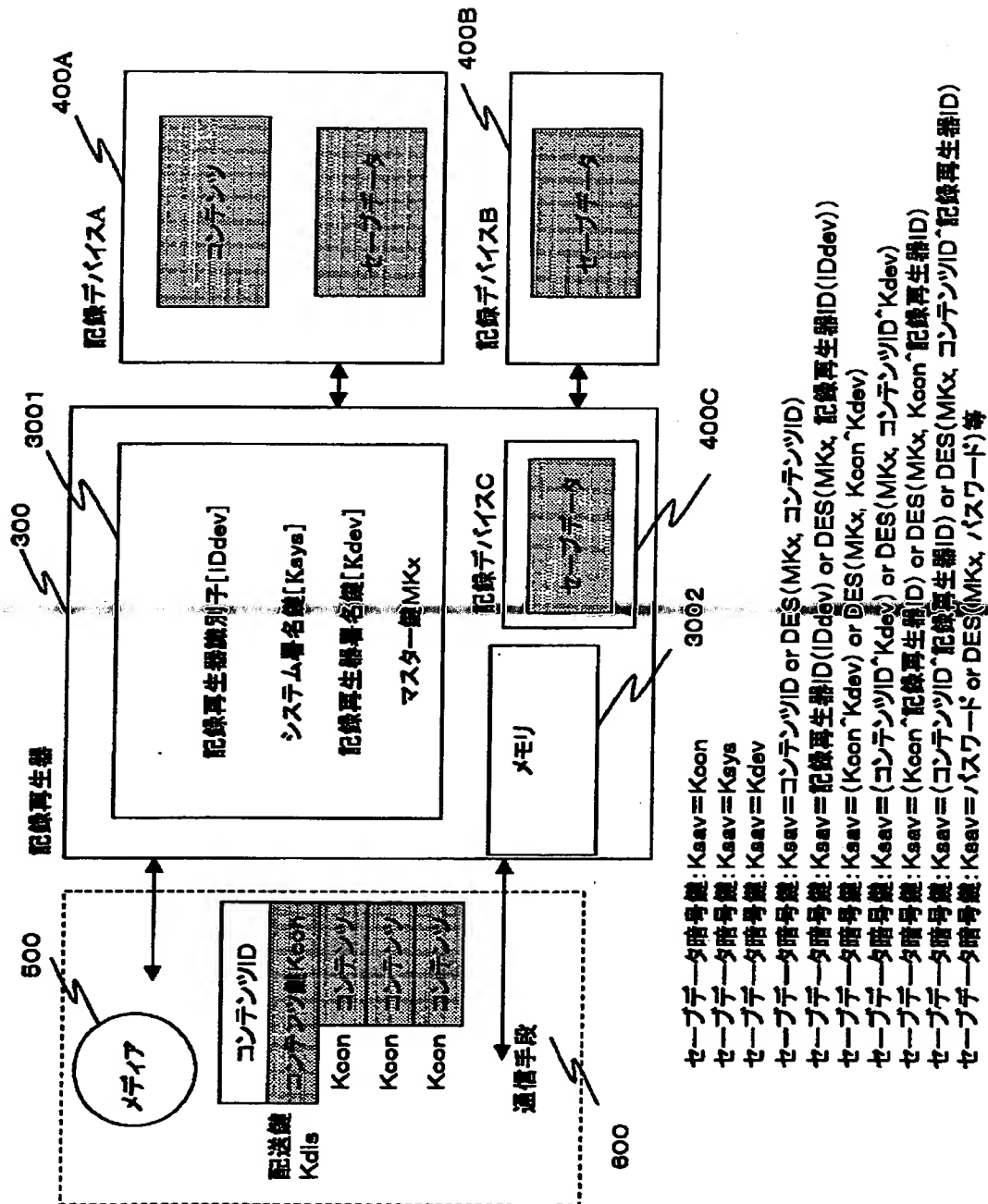
コンテンツ構成例(4)



【図 68】

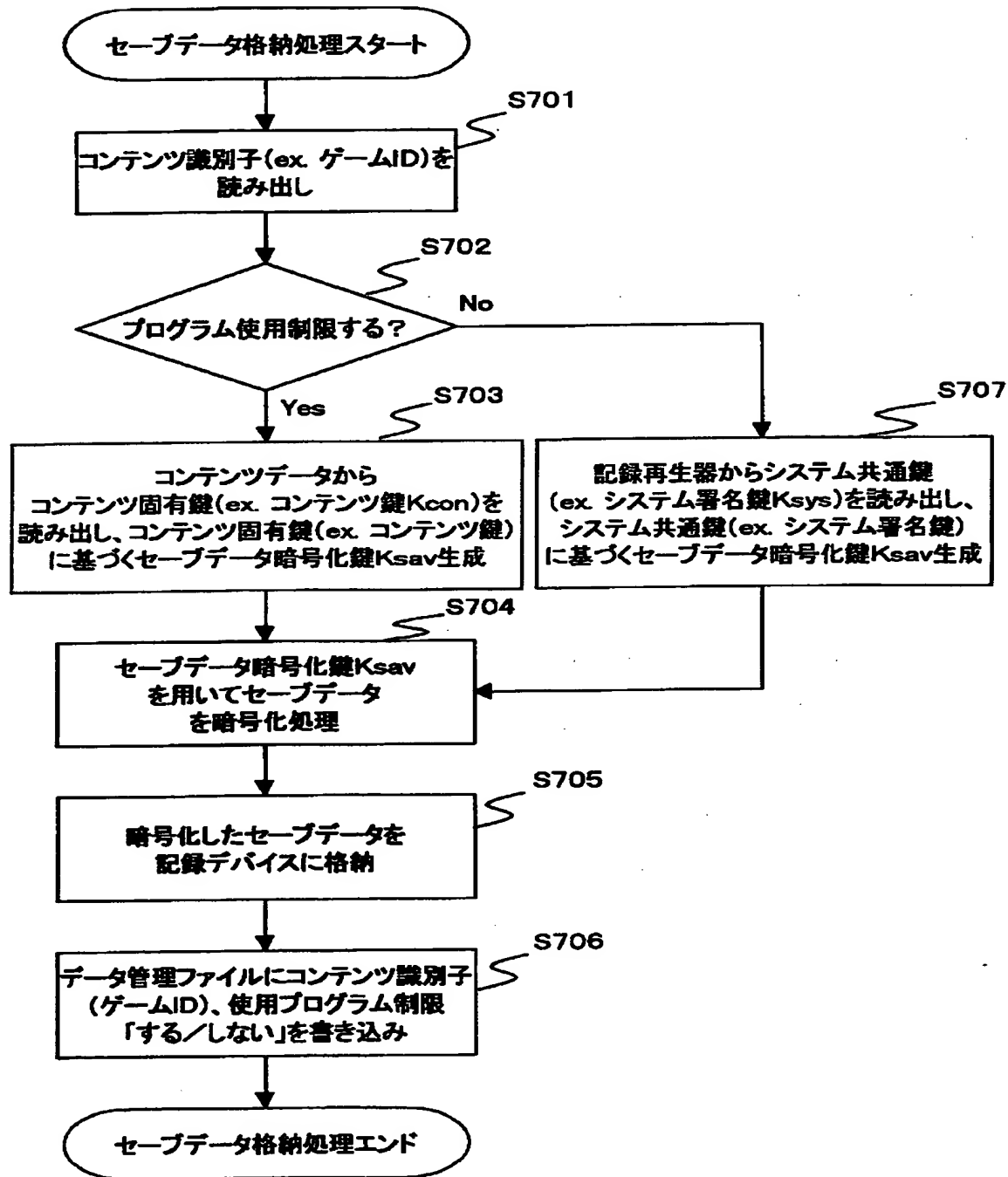


【図 69】



【図 70】

(1)コンテンツ固有鍵、orシステム共通鍵を使用したセーブデータ格納処理例



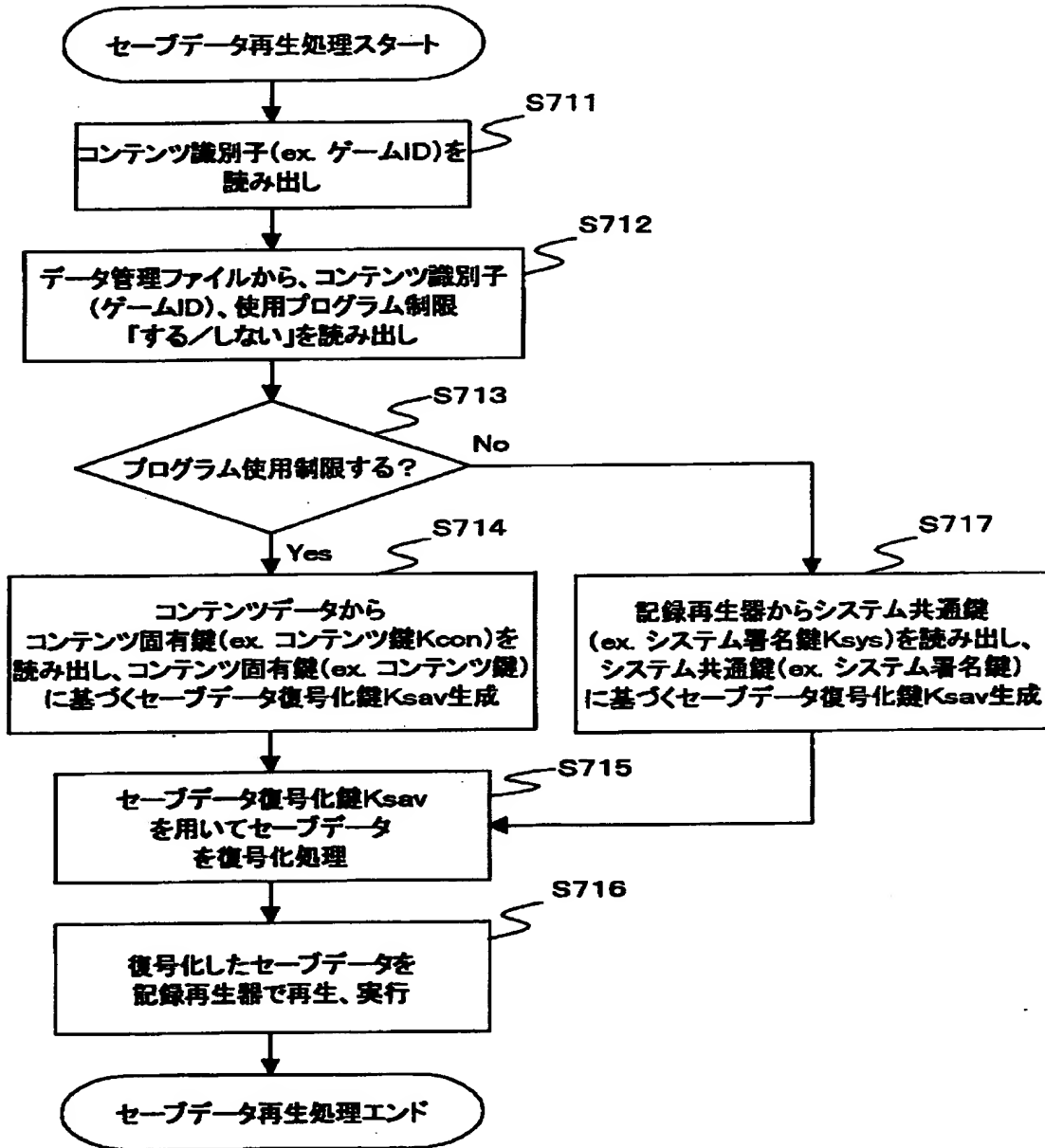
【図 7 1】

データ管理ファイル(1)

| データ番号 | コンテンツ識別子 (ゲームID) | 記録再生器識別子 (IDdev) | プログラム使用制限 |
|-------|---------------------|---------------------|-----------|
| 1 | 12345678... | 56789012... | する |
| 2 | ABCDEF12... | 09876543... | する |
| 3 | 122457678... | 58834762... | しない |
| : | : | : | : |

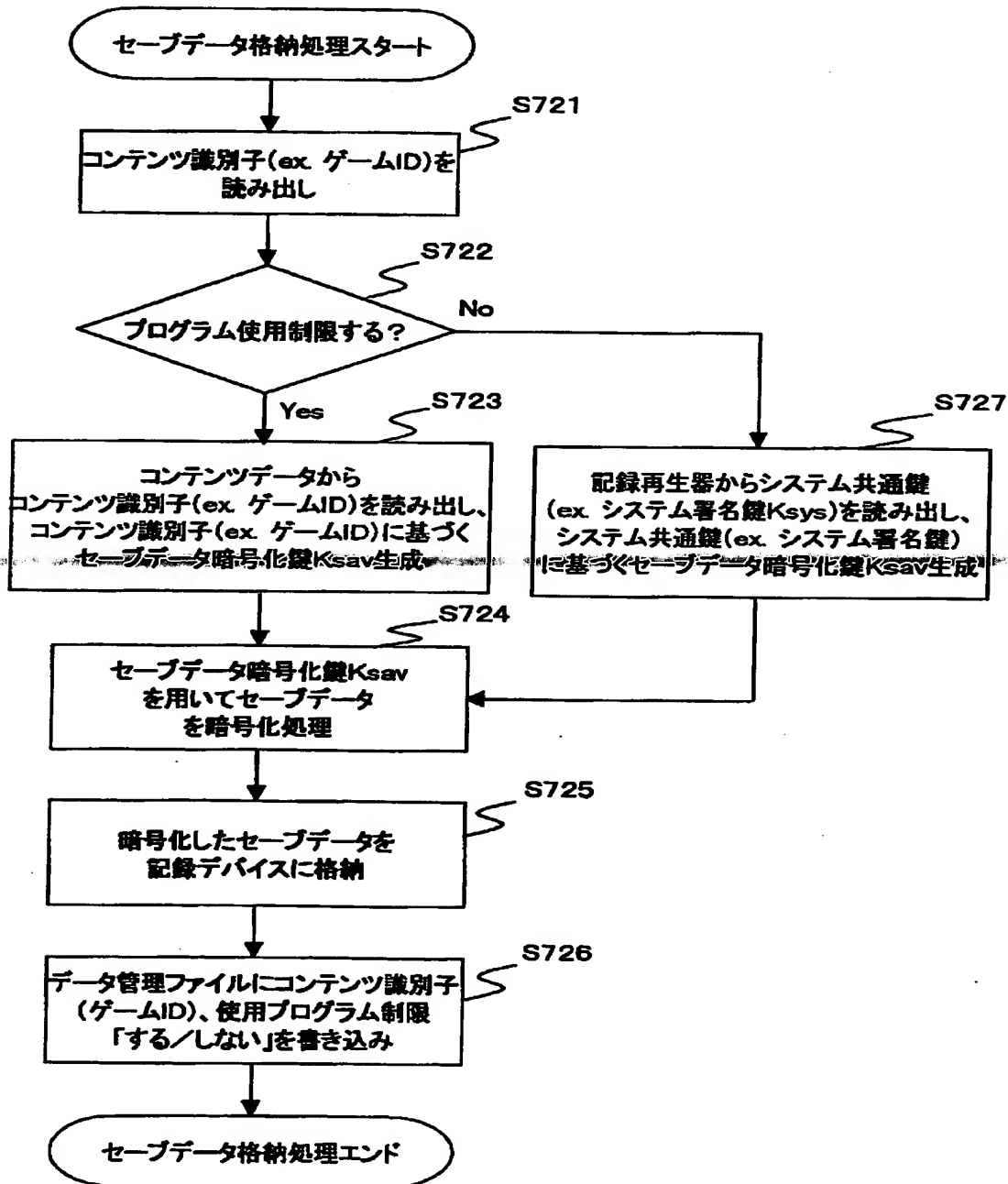
【図 7 2】

(2)コンテンツ固有鍵、orシステム共通鍵を使用したセーブデータ再生処理例



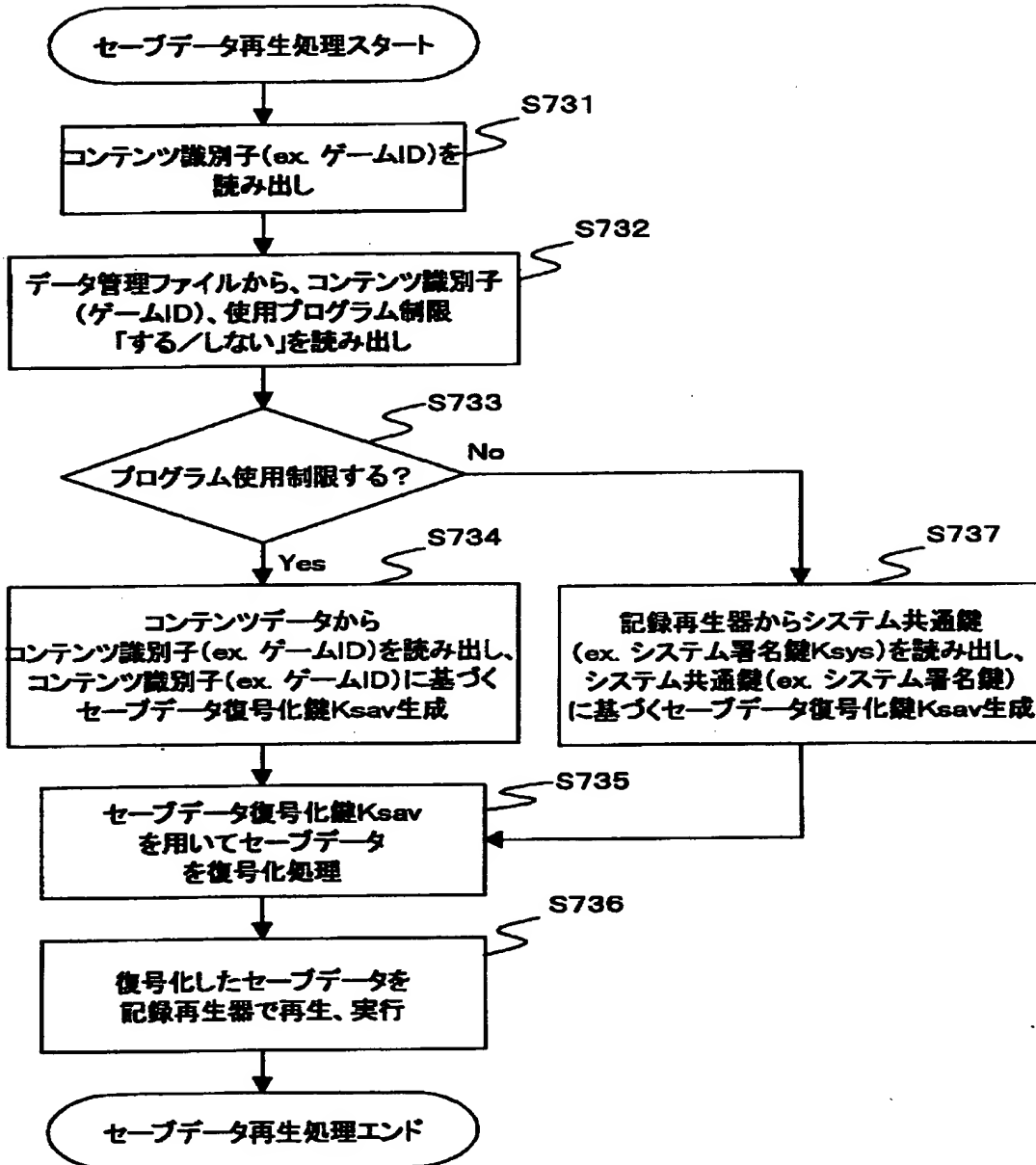
【図 7 3】

(3)コンテンツID、orシステム共通鍵を使用したセーブデータ格納処理例



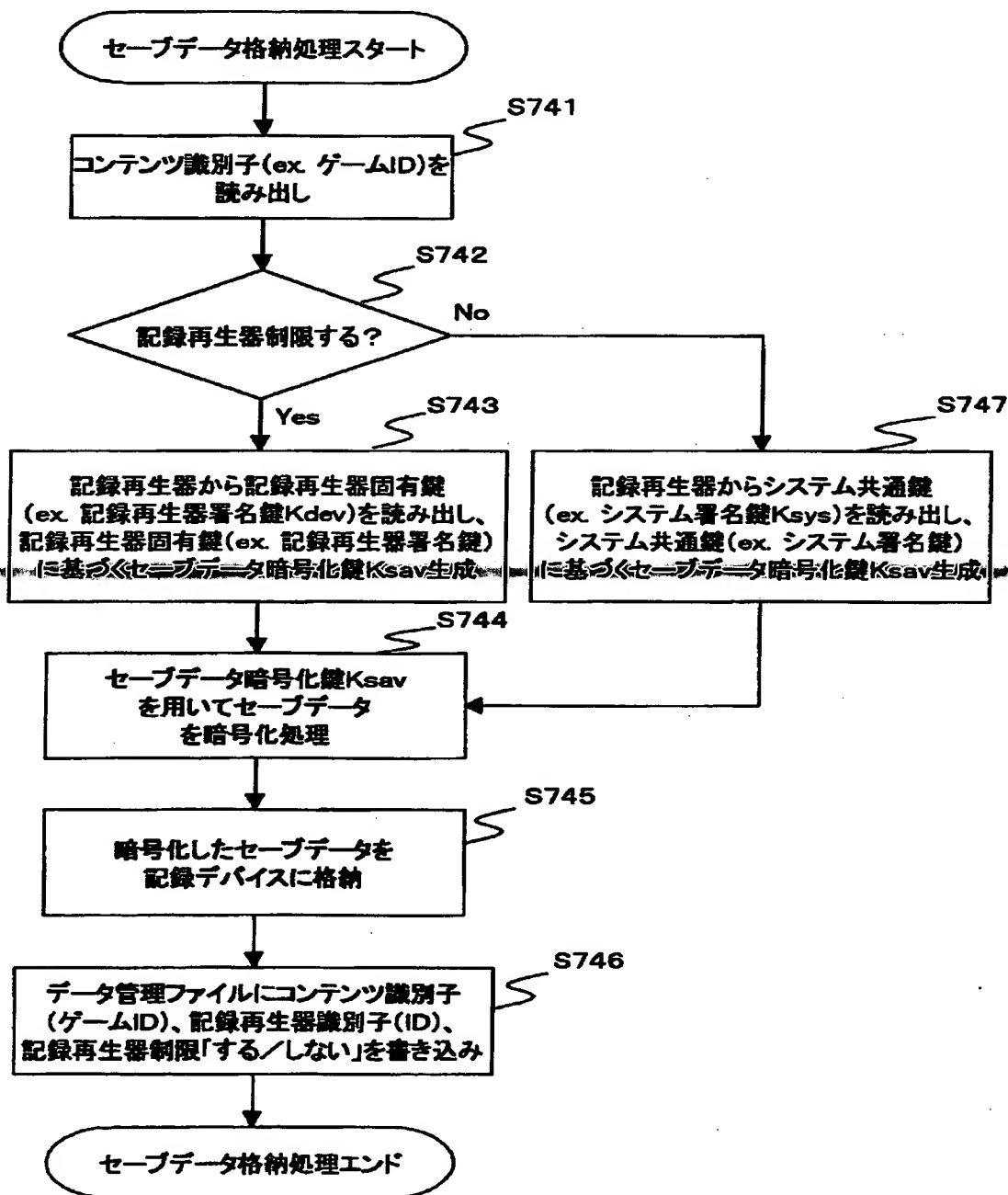
【図74】

(4)コンテンツID、orシステム共通鍵を使用したセーブデータ再生処理例



【図75】

(5)記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例



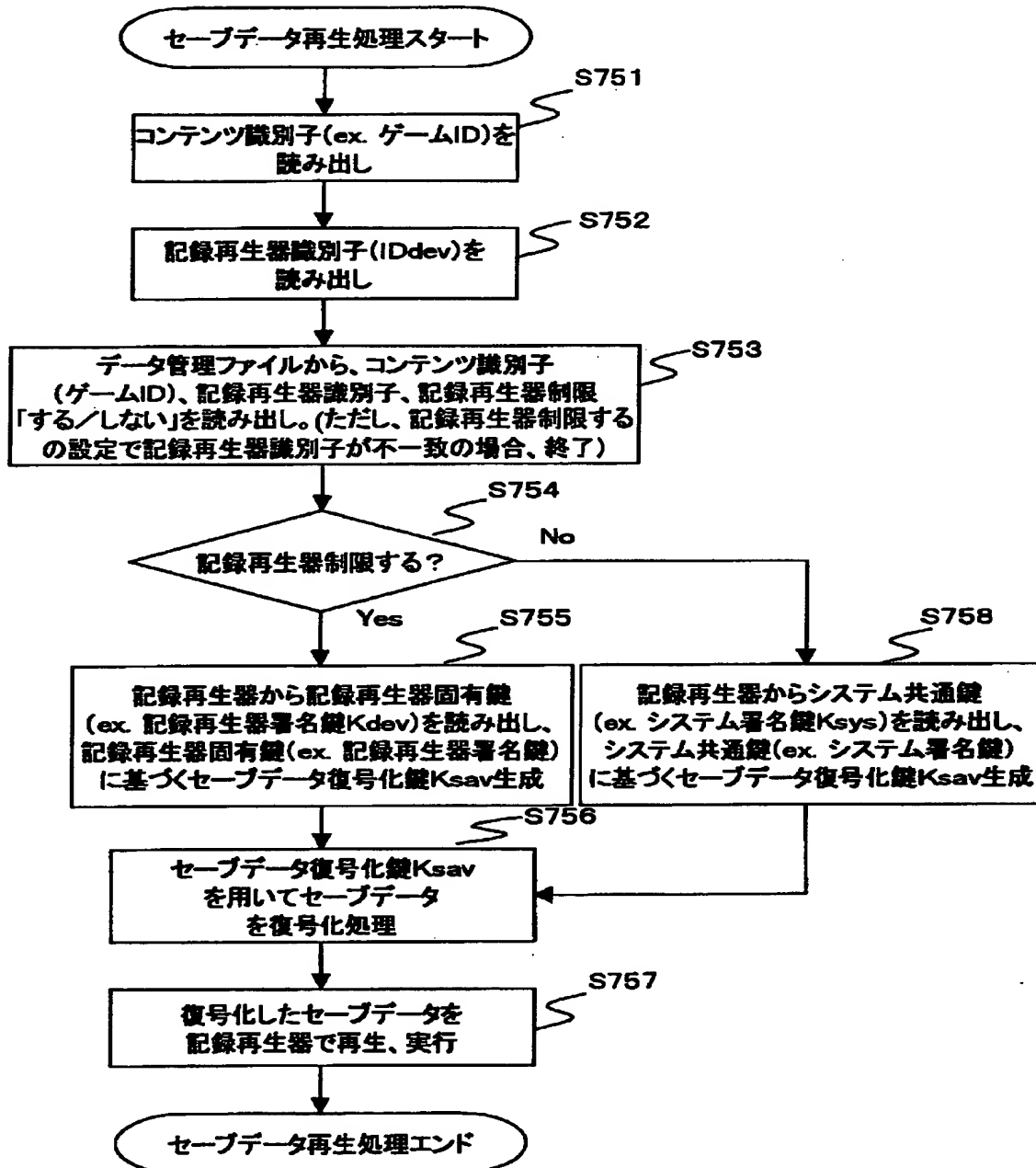
【図 76】

データ管理ファイル(2)

| データ番号 | コンテンツ識別子 (ゲームID) | 記録再生器識別子 (IDdev) | 記録再生器制限 |
|-------|---------------------|---------------------|---------|
| 1 | 12345678... | 56789012... | しない |
| 2 | ABCDEF12... | 09876543... | する |
| 3 | 122457678... | 58834762... | する |
| : | : | : | : |

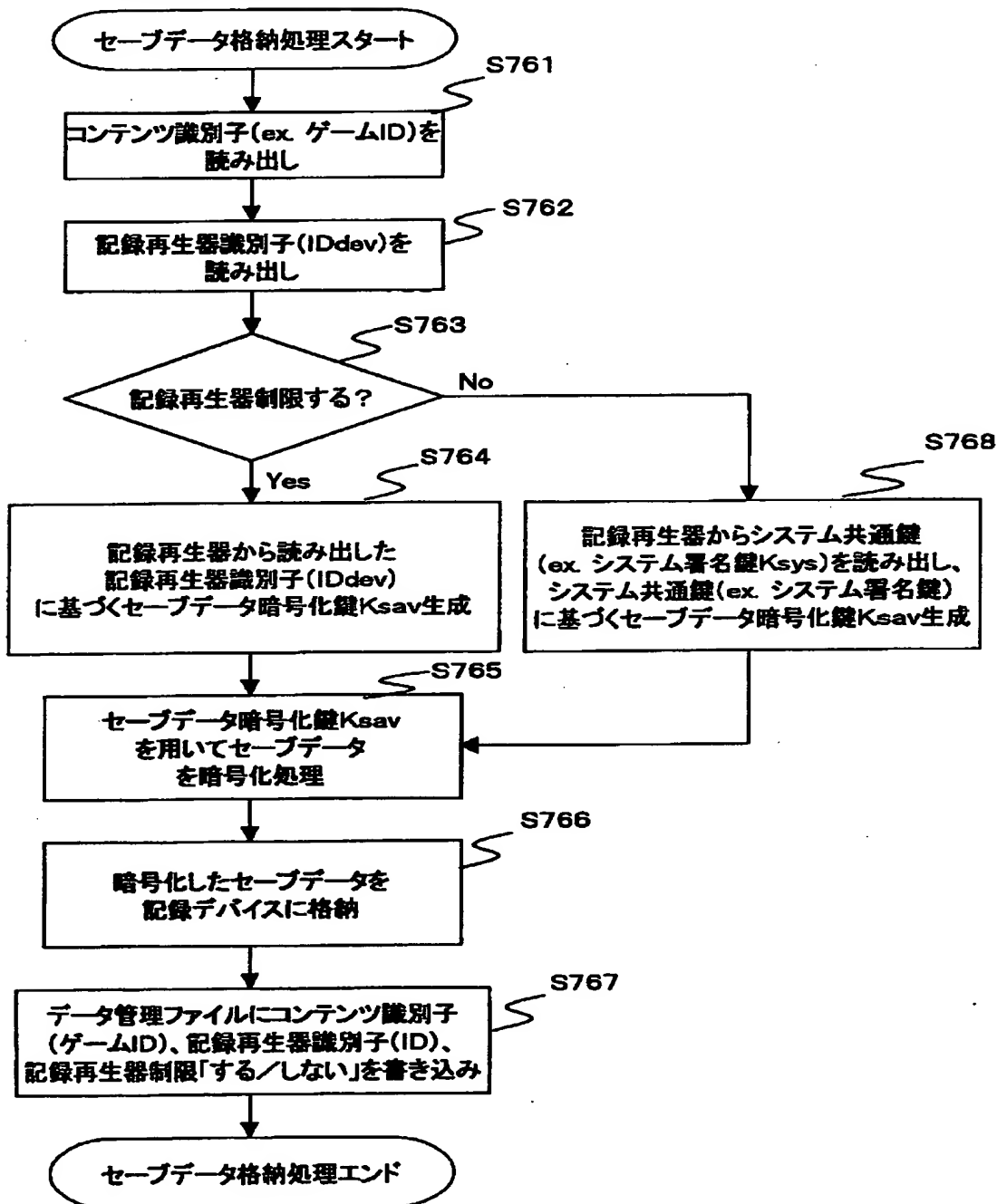
【図 77】

(6) 記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例



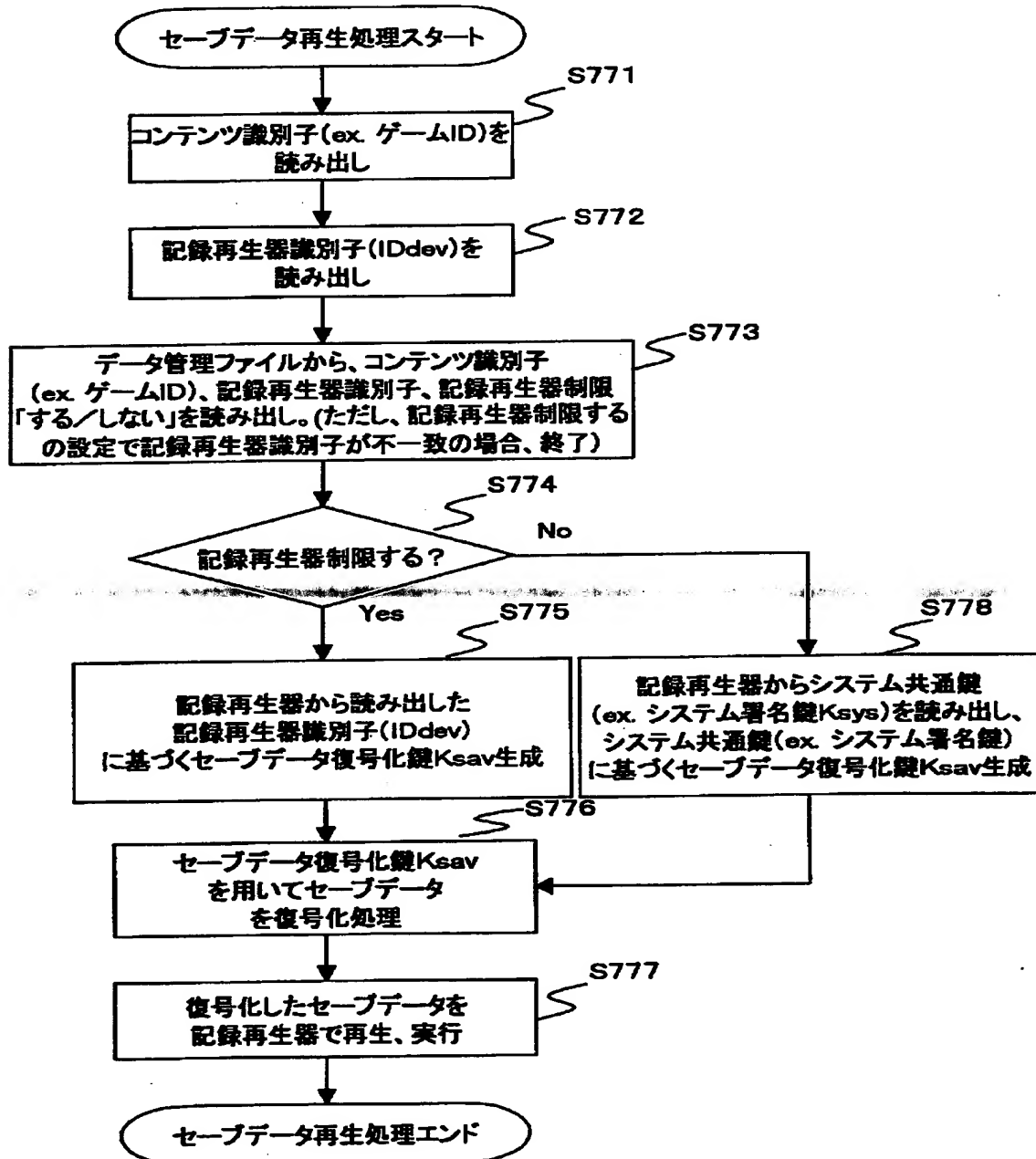
【図 78】

(7)記録再生器識別子、or システム共通鍵を使用したセーブデータ格納処理例



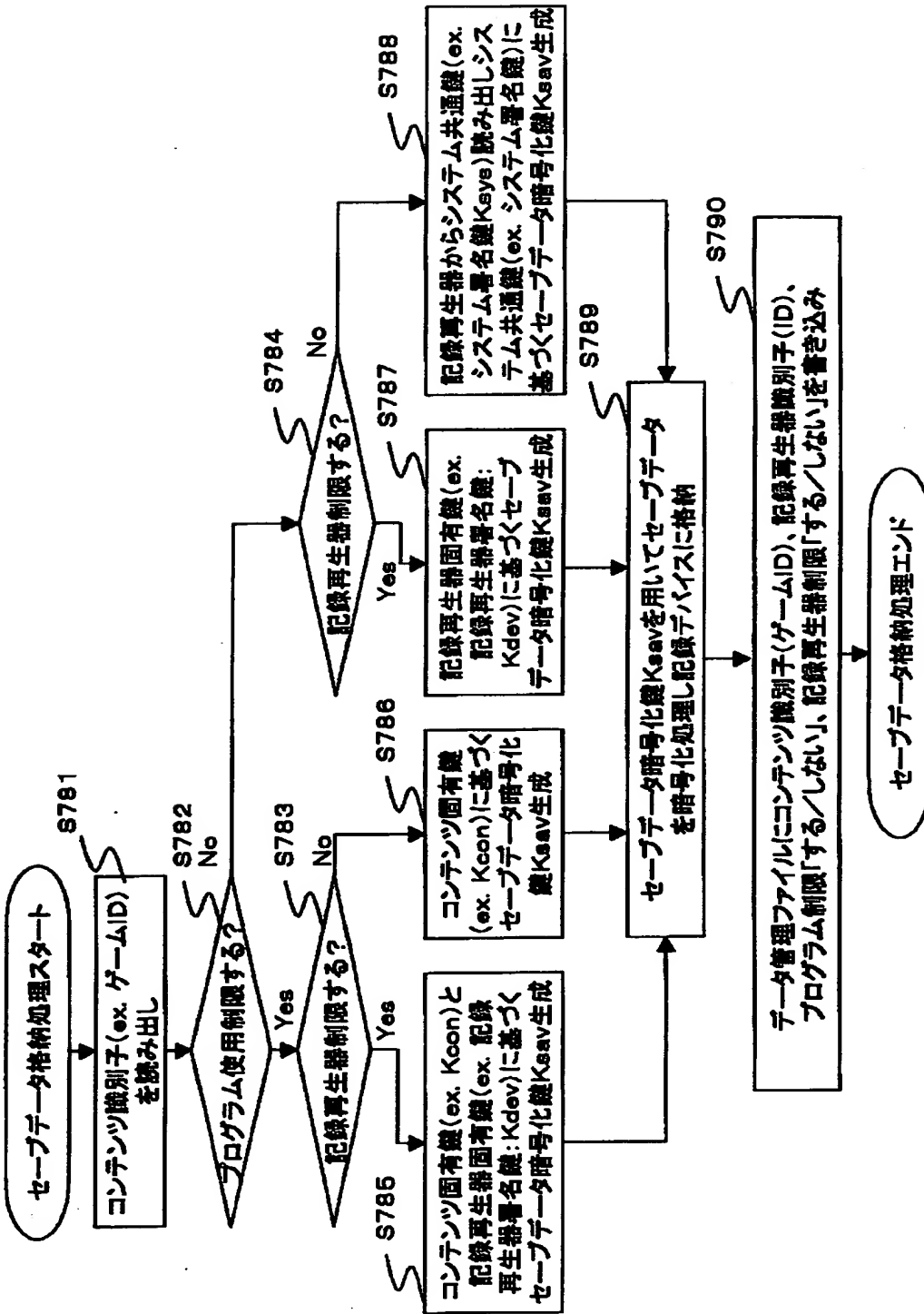
【図 79】

(8)記録再生器識別子、or システム共通鍵を使用したセーブデータ再生処理例



【図 80】

(9)コンテンツ固有鍵、記録再生器固有鍵、or システム共通鍵を使用したセーブデータ格納処理例



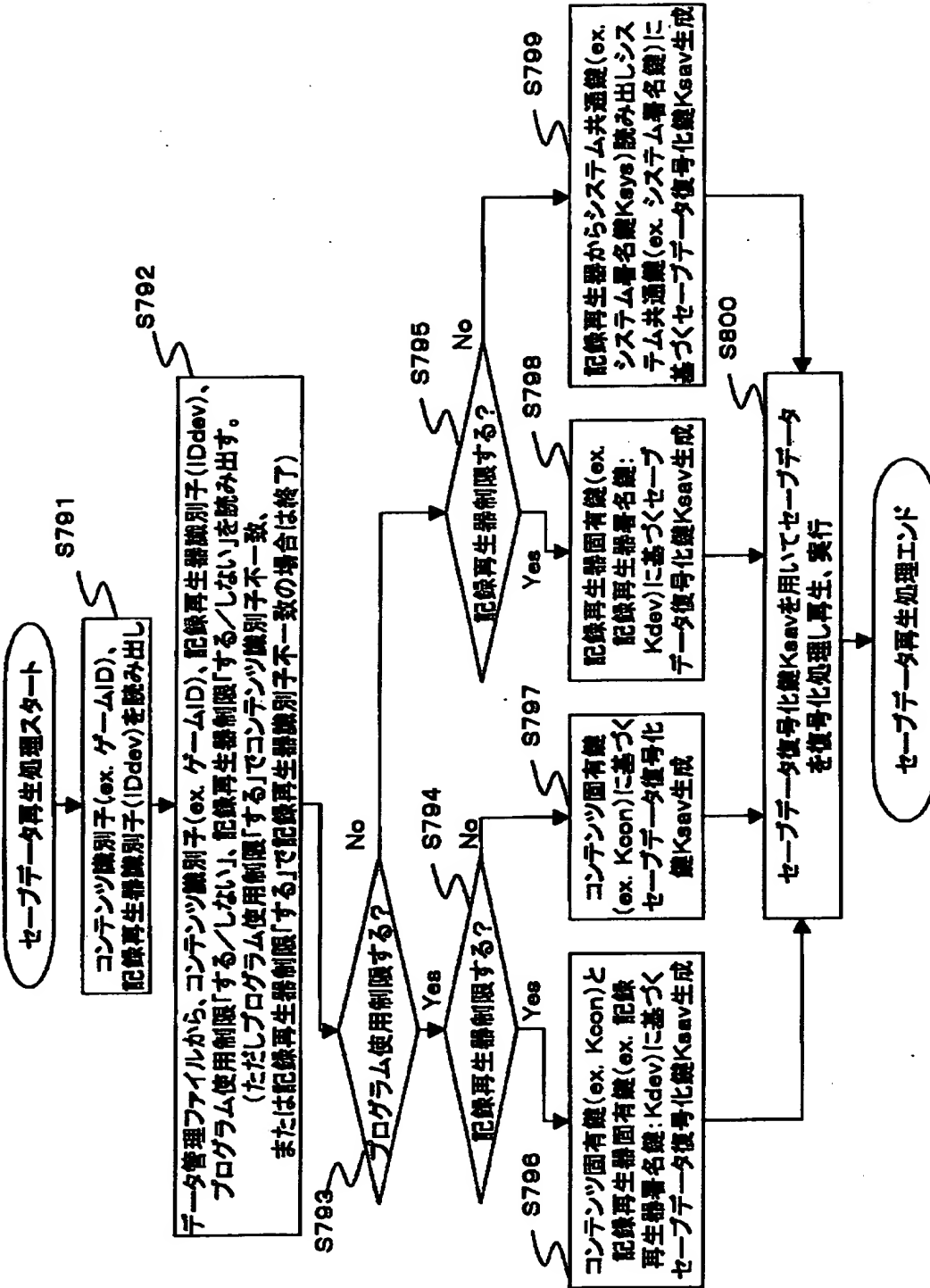
【図 8 1】

データ管理ファイル(3)

| データ番号 | コンテンツ識別子 (ゲームID) | 記録再生器識別子 (IDdev) | プログラム使用制限 | 記録再生器制限 |
|-------|---------------------|---------------------|-----------|---------|
| 1 | 12345678... | 56789012... | する | しない |
| 2 | ABCDEF12... | 09876543... | する | する |
| 3 | 122457678... | 58834762... | しない | する |
| : | : | : | : | : |

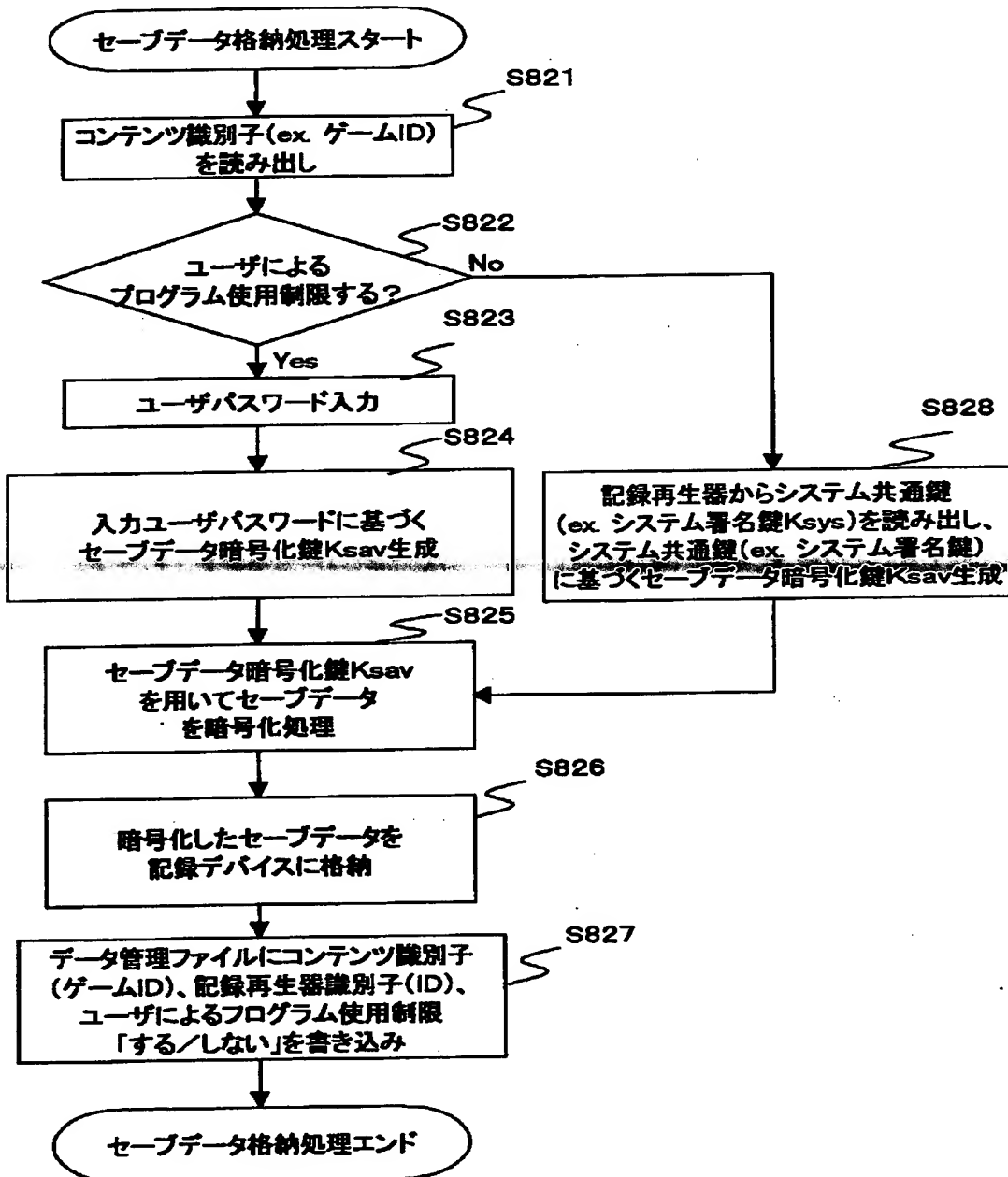
【図 82】

(10)コンテンツ固有鍵、記録再生器固有鍵、or システム共通鍵を使用したセーブデータ再生処理例



【図 83】

(11) ユーザパスワード、or システム共通鍵を使用したセーブデータ格納処理例



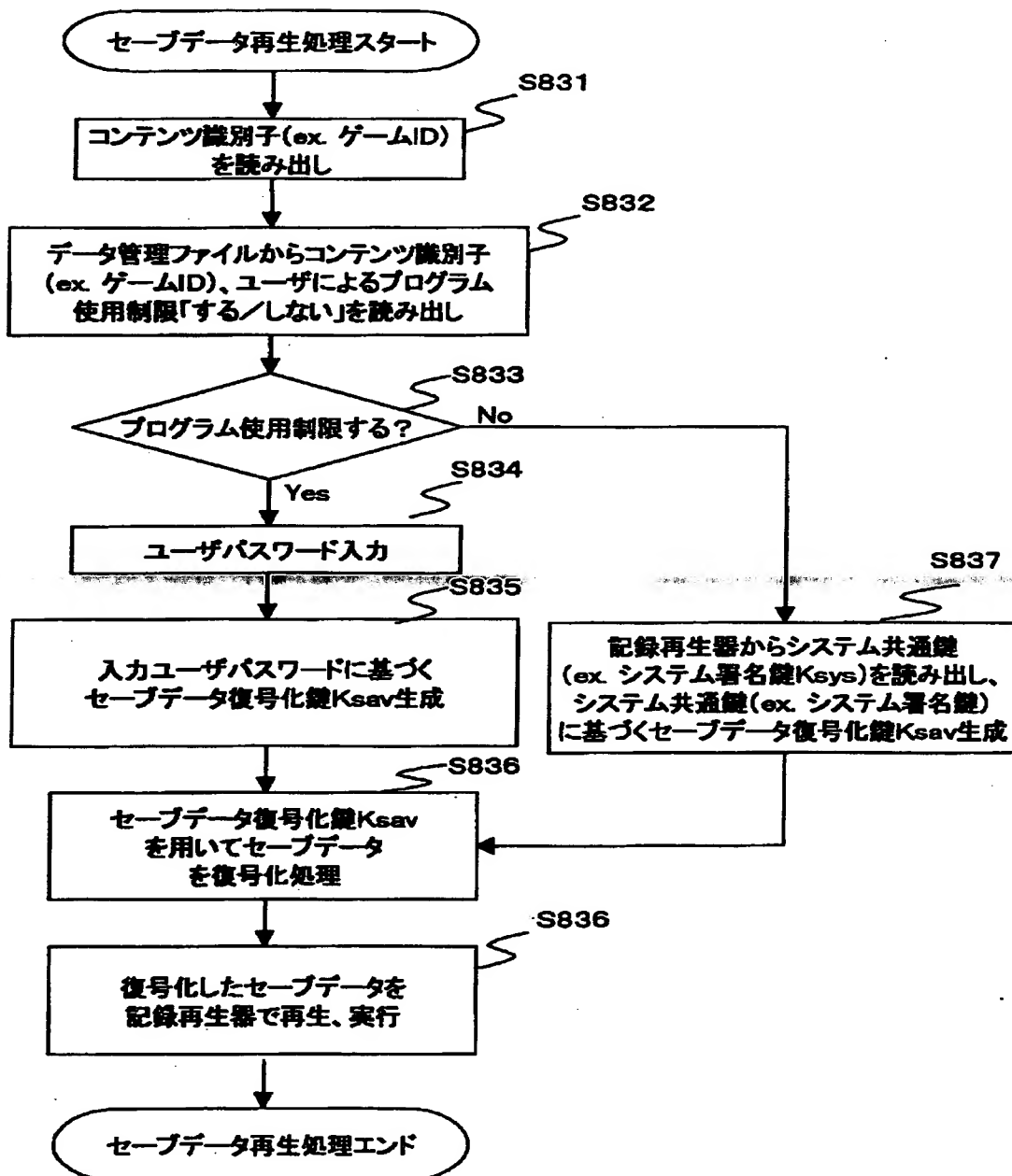
【図 84】

データ管理ファイル(4)

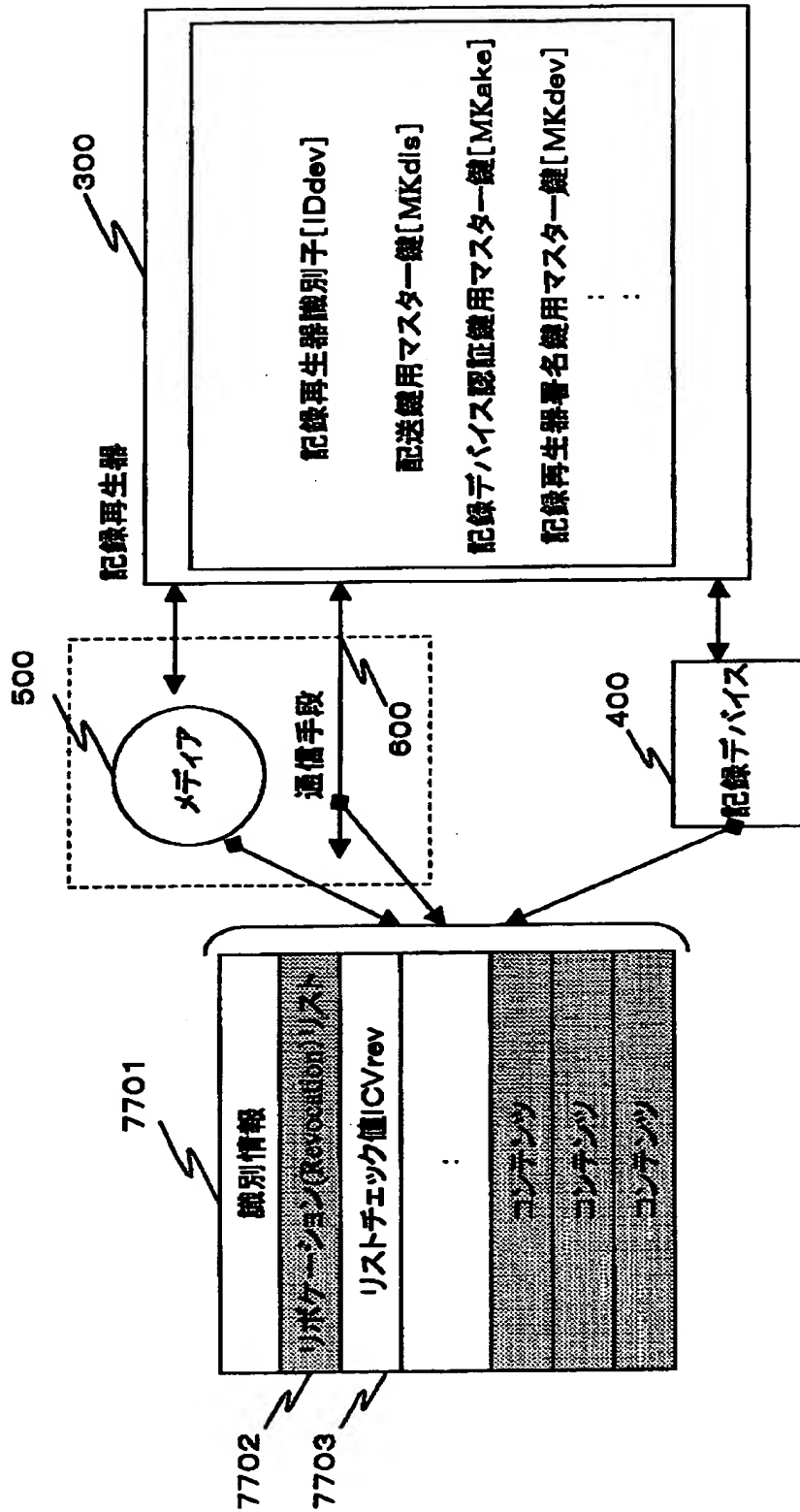
| データ番号 | コンテンツ識別子 (ゲームID) | 記録再生器械別子 (IDdev) | ユーザによる プログラム使用制限 |
|-------|---------------------|---------------------|---------------------|
| 1 | 12345678... | 56789012... | する |
| 2 | ABCDEF12... | 09876543... | する |
| 3 | 122457678... | 58834762... | しない |
| : | : | : | : |

【図85】

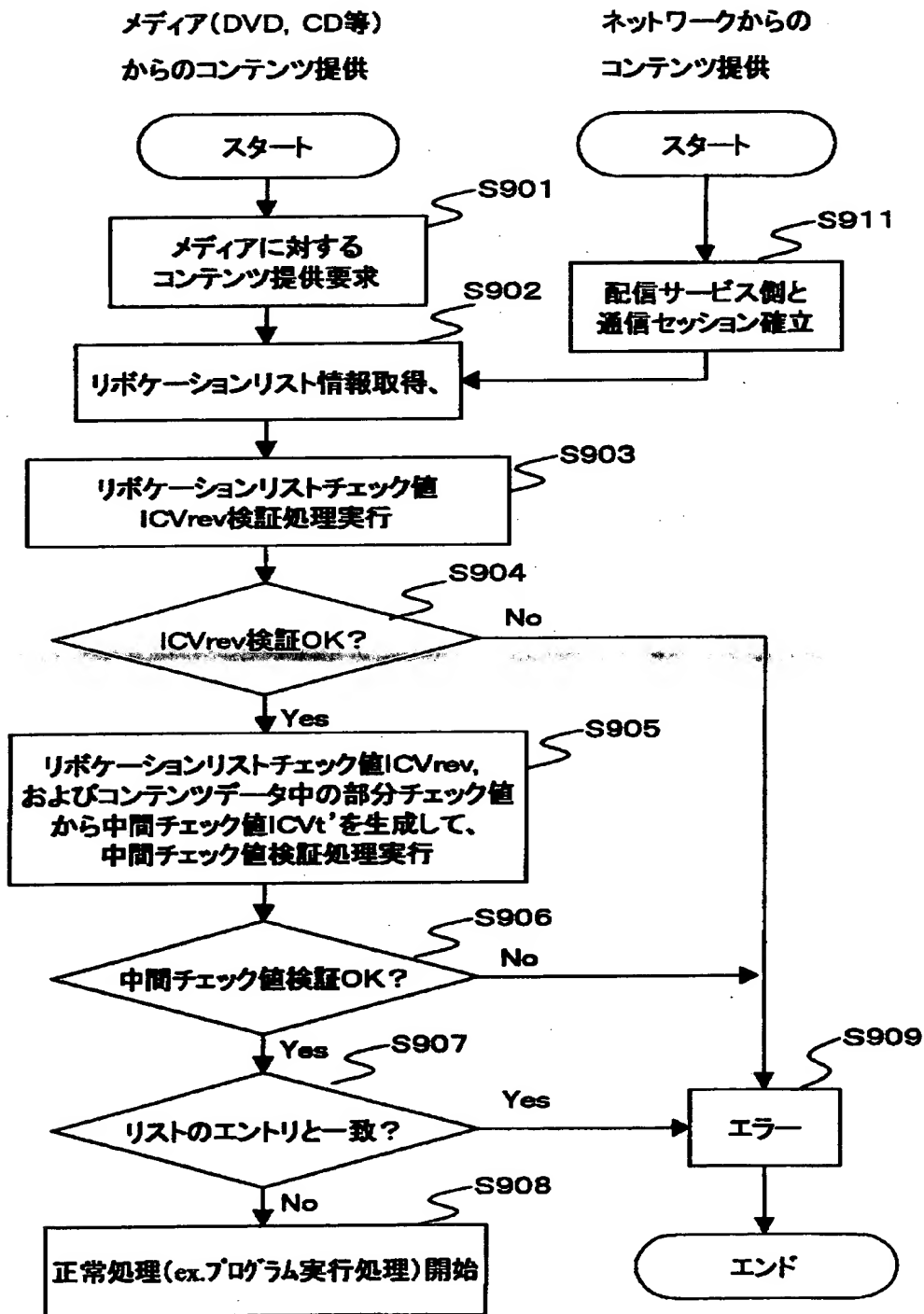
(12) ユーザパスワード、or システム共通鍵を使用したセーブデータ再生処理例



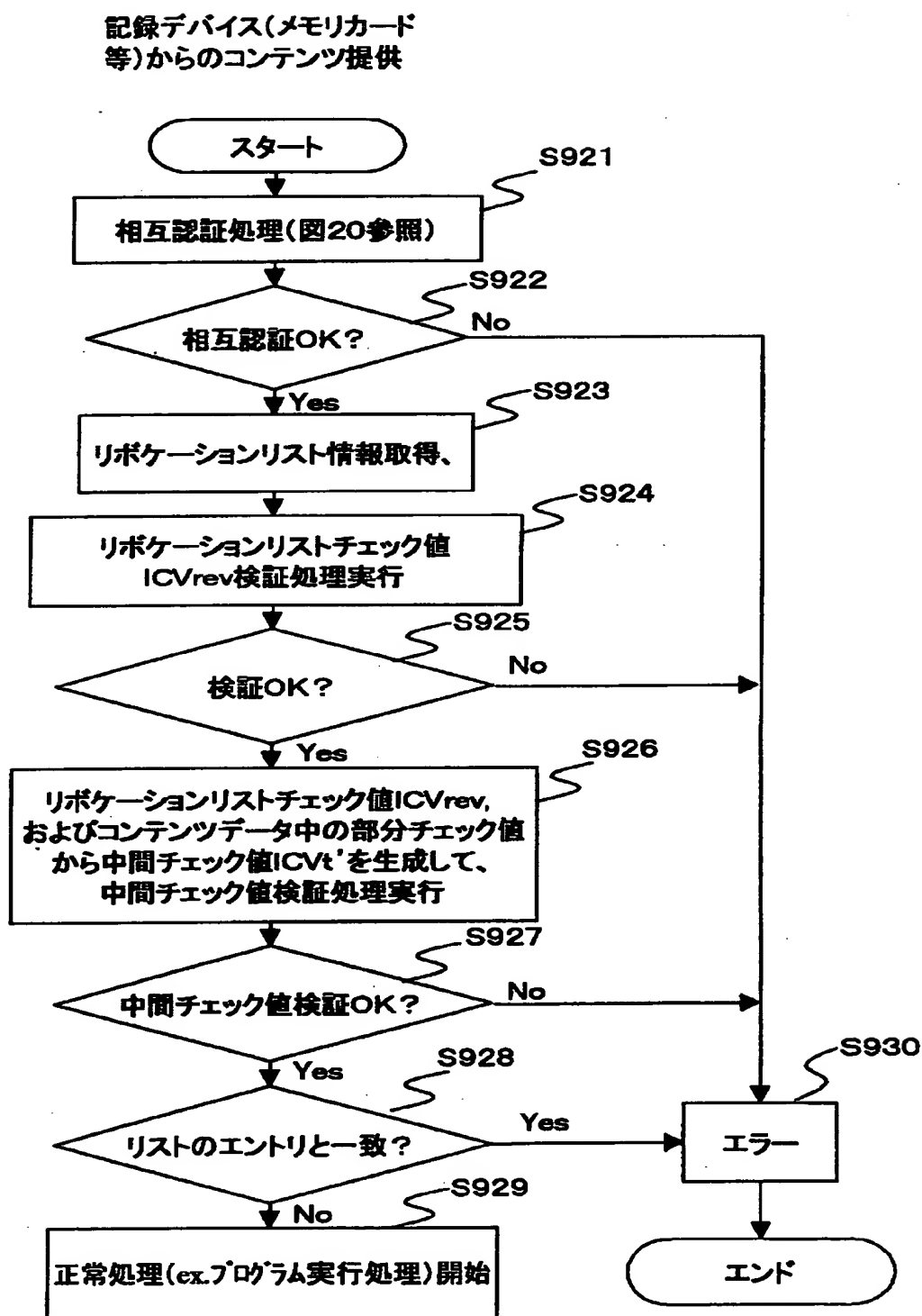
【図 86】



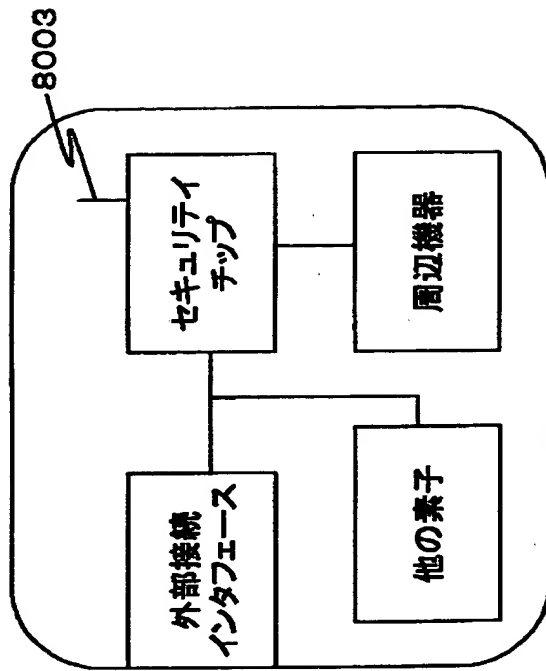
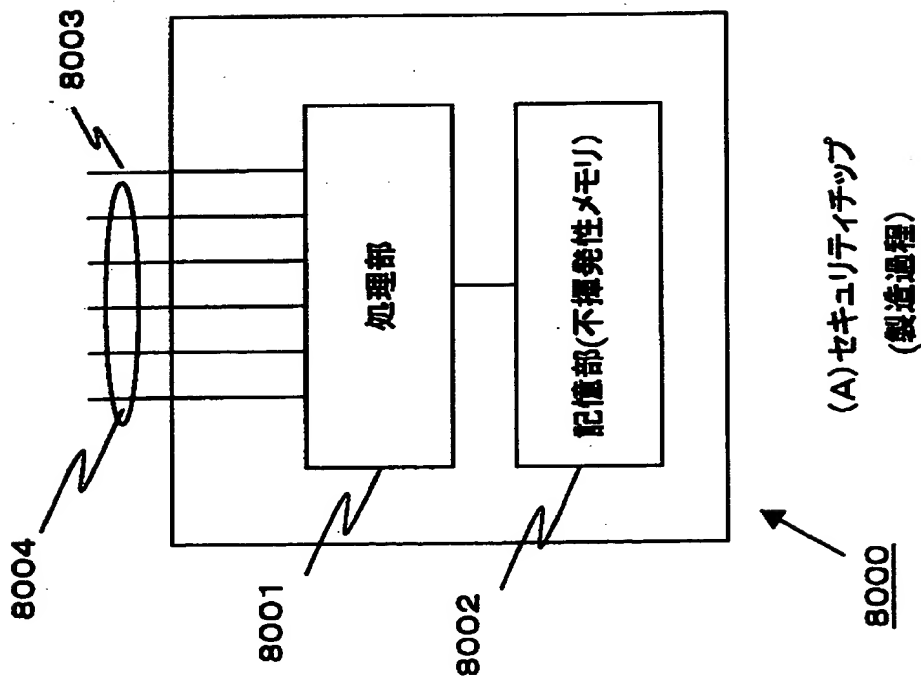
【図 87】



【図 88】

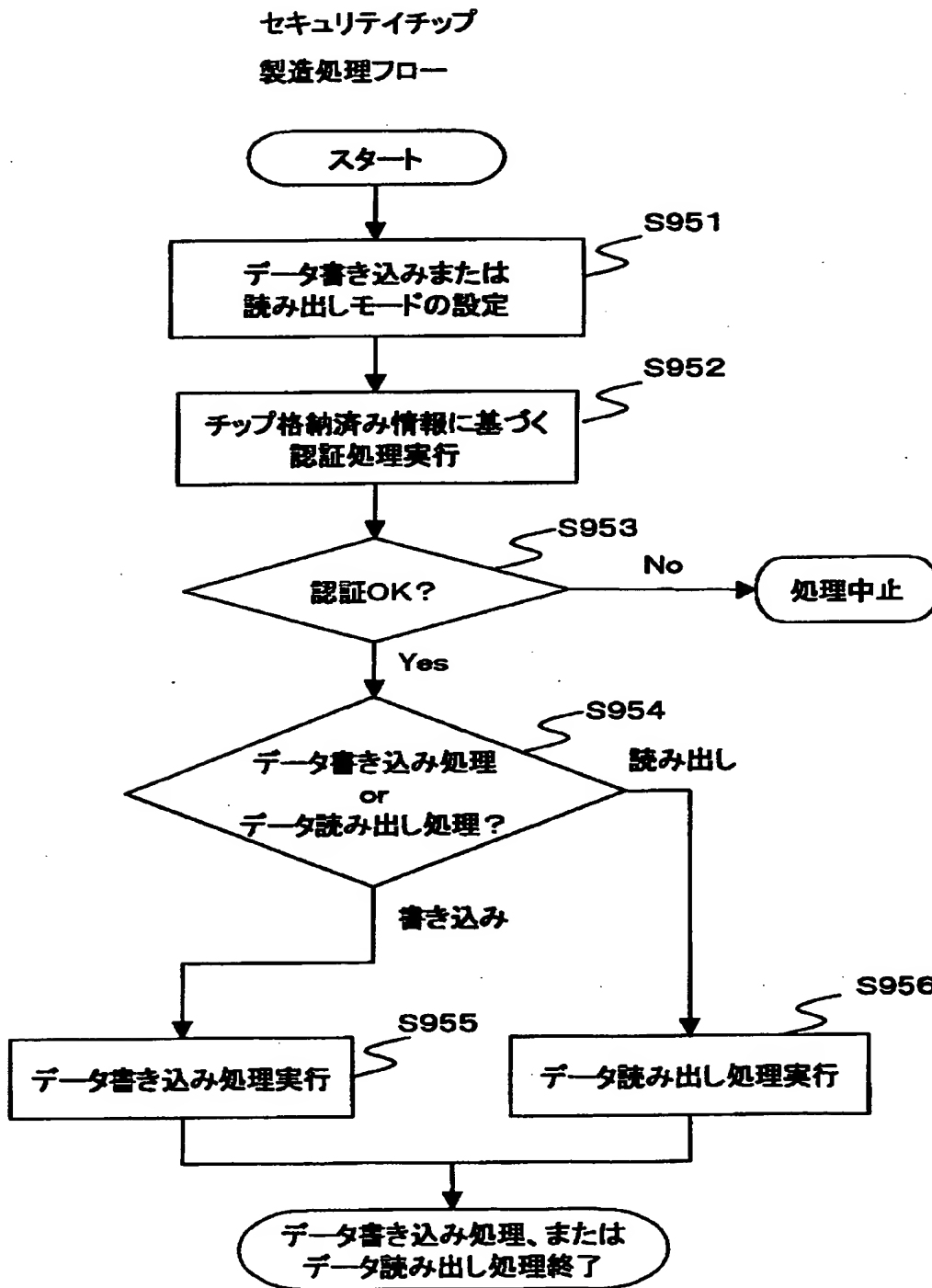


【図 89】

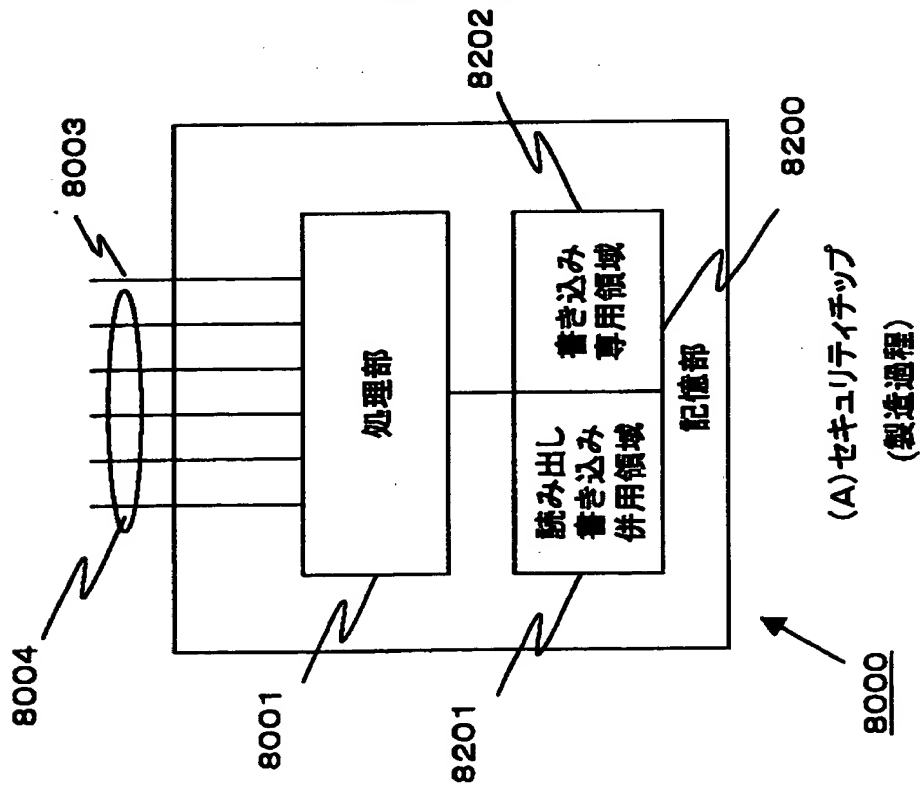


(B)セキュリティチップ搭載製品
(ex. 記録再生器、記録デバイス)

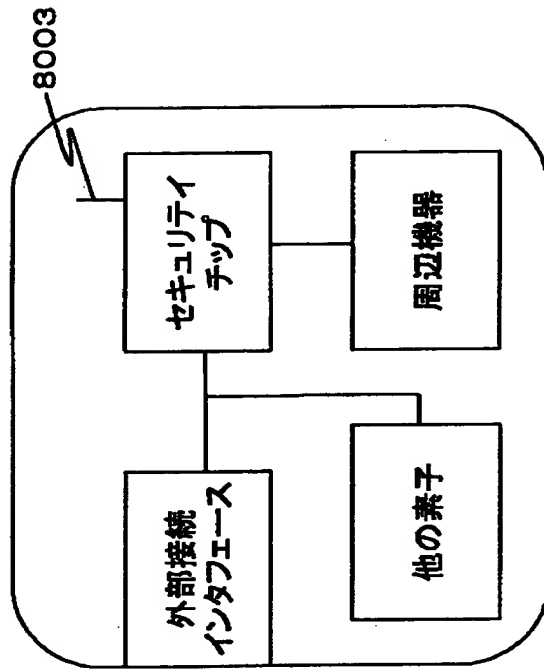
【図90】



【図 91】

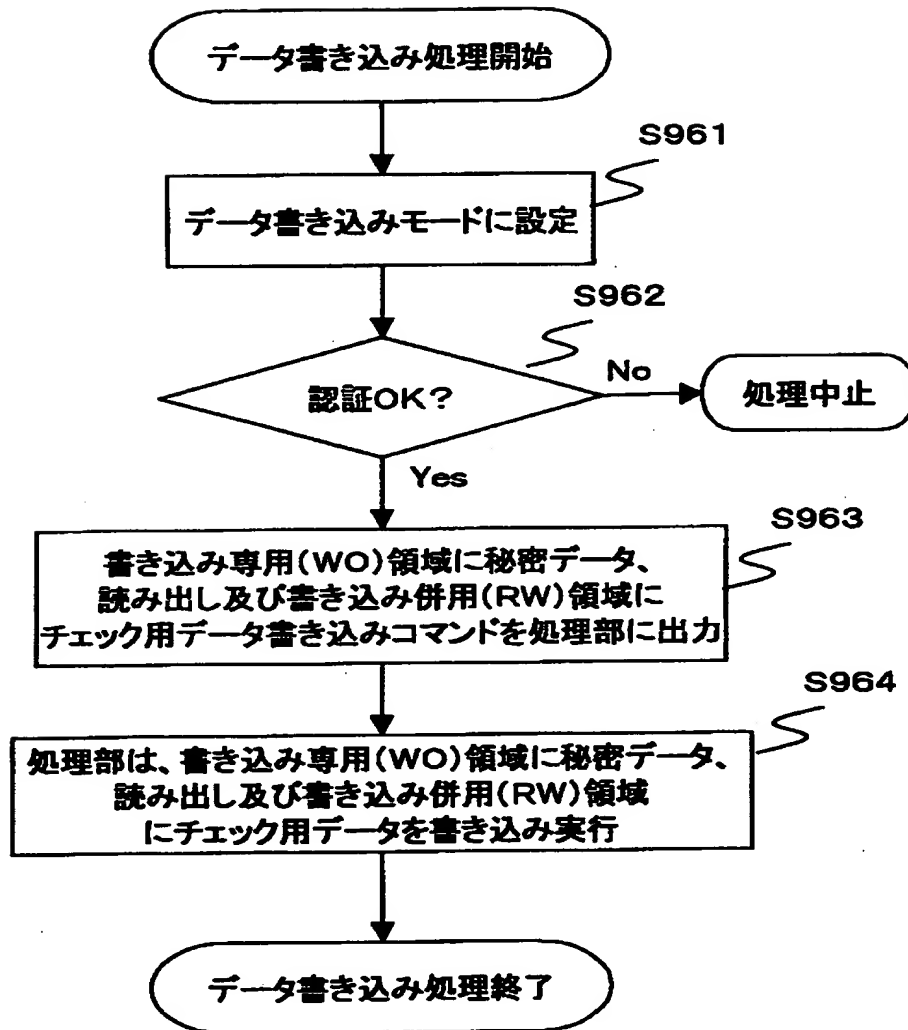


(A)セキュリティチップ
(製造過程)

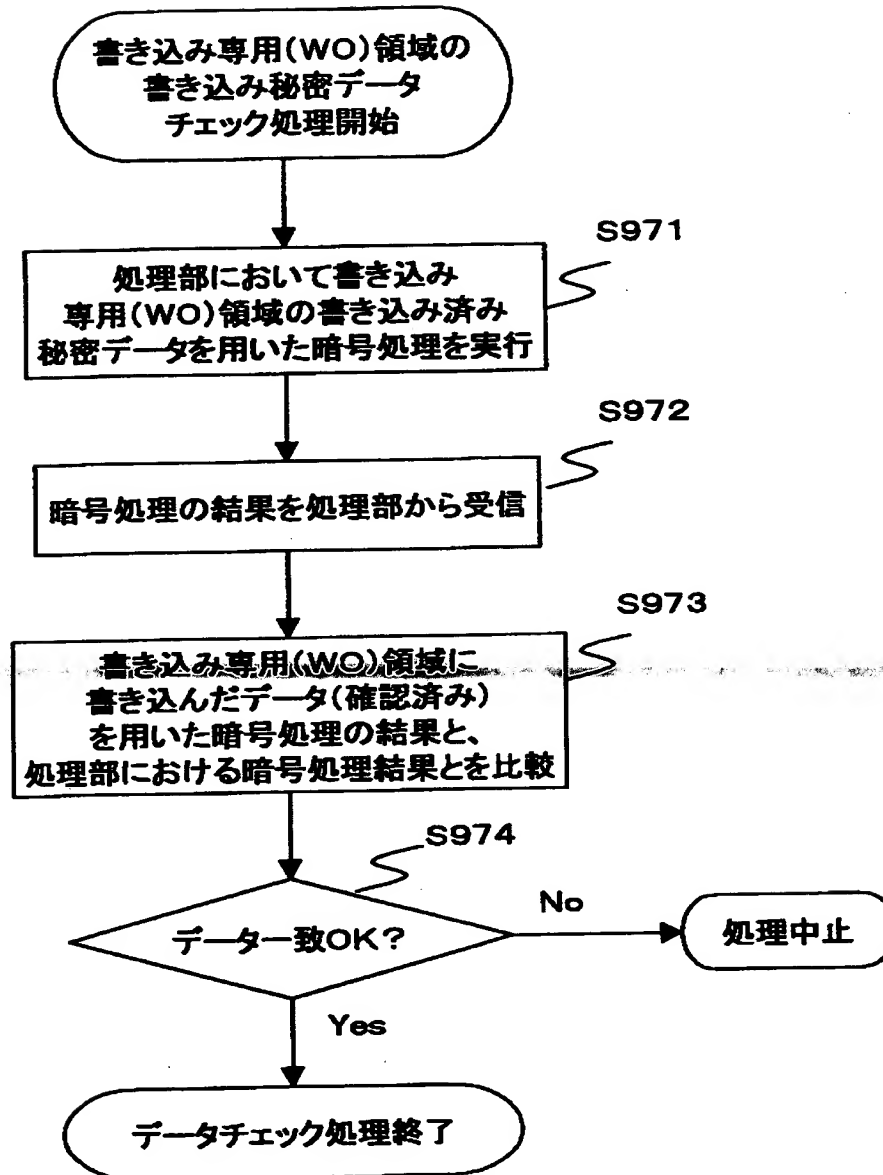


(B)セキュリティチップ搭載製品
(ex. 記録再生器、記録デバイス)

【図 9 2】



【図93】



【書類名】 要約書

【要約】

【課題】 暗号処理におけるセキュリティ、特に暗号処理用鍵データの漏洩を防止したデータ処理装置を提供する。

【解決手段】 データ処理装置において、データ暗号化、データ復号化、データ検証、認証処理、署名処理等の暗号処理を実行するために必要となる個別鍵を記憶部に格納せず、これらの個別鍵を生成するためのマスター鍵を記憶部に格納する。データ処理装置の暗号処理部は、暗号鍵、認証鍵等の個別鍵を必要に応じて生成する。個別鍵に対応するマスター鍵を記憶部から取り出し、取り出したマスター鍵と、装置またはデータの識別データに基づいて、例えばDESアルゴリズムを適用した暗号処理を実行して、暗号鍵、認証鍵等の個別鍵を生成する。

【選択図】 図 4 9

出 願 人 履 歴 情 報

識別番号

[000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社